JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2024, 1–18
https://doi.org/10.1093/cybsec/tyad023

Review Article

A systematic literature review on advanced persistent threat behaviors and its detection strategy

Nur Ilzam Che Mat [1,*], Norziana Jamil [2,1,*], Yunus Yusoff [1], Miss Laiha Mat Kiah [3]

[1]Institute of Informatics and Computing in Energy (IICE) and College of Computing and Informatics, University Tenaga Nasional, 43000 Kajang, Malaysia
[2]College of IT, United Arab Emirates University, P.O. Box 15551, Al Ain, Abu Dhabi, UAE
[3]Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia

*Corresponding author. College of IT, United Arab Emirates University, P.o. Box 1555, Al Ain, Abu Dhabi, UAE. Phone: +971-3-7673333. E-mail: Norziana@uaeu.ac.ae

Received 18 July 2022; revised 29 August 2023; accepted 22 September 2023

Abstract

Advanced persistent threats (APTs) pose significant security-related challenges to organizations owing to their sophisticated and persistent nature, and are inimical to the confidentiality, integrity, and availability of organizational information and services. This study systematically reviews the literature on methods of detecting APTs by comprehensively surveying research in the area, identifying gaps in the relevant studies, and proposing directions for future work. The authors provide a detailed analysis of current methods of APT detection that are based on multi-stage attack-related behaviors. We adhered to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines and conducted an extensive search of a variety of databases. A total of 45 studies, encompassing sources from both academia and the industry, were considered in the final analysis. The findings reveal that APTs have the capability to laterally propagate and achieve their objectives by identifying and exploiting existing systemic vulnerabilities. By identifying shortcomings in prevalent methods of APT detection, we propose integrating the multi-stage attack-related behaviors of APTs with the assessment of the presence of vulnerabilities in the network and their susceptibility to being exploited in order to improve the accuracy of their identification. Such an improved approach uses vulnerability scores and probability metrics to determine the probable sequence of targeted nodes, and visualizes the path of APT attacks. This technique of advanced detection enables the early identification of the most likely targets, which, in turn, allows for the implementation of proactive measures to prevent the network from being further compromised. The research here contributes to the literature by highlighting the importance of integrating multi-stage attack-related behaviors, vulnerability assessment, and techniques of visualization for APT detection to enhance the overall security of organizations.

Keywords: systematic literature review; PRISMA; advanced persistent threat; APT mitigation technique; multi-stage attack; detection technique; energy security

Introduction

Cybercriminals continue to develop increasingly sophisticated attack tools despite advances in enterprise security technologies, such as anti-viruses and firewalls, to detect and stop cyberattacks [1, 2]. According to Cinar et al. and Blumbergs [3, 4], many strategies to protect against cyberattacks assume that the attacker randomly targets networks. If a network has adequate defensive capabilities, the attacker gives up and moves on to a less complicated target. However, research by Micro and Report [5] has shown that this assumption is no longer viable due to the development of an advanced and targeted

form of attack known as advanced persistent threat (APT). The APT selects a target regardless of its defenses and persists until it breaches them. APTs have mainly been used to target critical infrastructures, such as electrical power grids. The Stuxnet attack in 2010 [6] and the Triton attack in 2017 are examples of APTs [7].

Recent research has examined APT attacks by analyzing indicators of compromise (IOCs), such as hash values, IP addresses, and attack tools [7, 8]. While such an approach can provide valuable insights into individual attacks, it often fails to capture the bigger picture of the operation and capabilities of APTs. Relying solely on IOCs leads to a neglect of important aspects of the behavior, tactics, and techniques of an APT, where this is crucial for understanding its modus operandi. Moreover, this approach may lead to APTs being confused with other cyberattacks and potentially leading to false alarms. Therefore, a more comprehensive approach is needed that can offer a better understanding of the behavior of an APT beyond simply the IOCs.

An APT applies different attack tools to ensure that it can remain undetected within the target network for months and even years [8]. The tools are consecutively used in different stages of the attack until they reach the target destination. The process begins with gaining access to a system and laterally progressing toward other segments of the network. Before the attempt to conceal harmful activity, a command and control (C&C) center provides instructions for how to carry out the attack [9, 10]. Various tactics, techniques, and procedures (TTPs) are used in each stage of an APT attack, which advances to the next stage. The term "tactics" refers to the method used by the APT to execute the attack from beginning to end. The techniques used by the APT during its attack are described as its technological "strategy" to achieve its targets. Finally, the "procedure" of an APT describes the steps used by the attacker to achieve its objectives. Because the TTP attribute can be used to profile an APT actor, it is useful to consider it as a component of a given technique of detection, and can be used to anticipate APT attacks and identify them early on.

Detecting APT attacks can be challenging owing to their elusive nature. Open-source intelligence (OSINT) is often used in the industry as a valuable tool for analyzing and verifying potential threats. OSINT can help identify APT groups and their TTPs by gathering threat-related information from publicly available sources, including those that may be used by APT attackers. This information can provide critical assistance in detecting APT attacks and support investigations into them. OSINT can also offer valuable insights into the methods and behaviors of APT groups, where this can help develop effective defensive strategies. For example, it can help organizations understand how APT groups operate, what tools and techniques they use, and how they typically gain access to the target system. Therefore, integrating OSINT into techniques of APT detection can help organizations better understand and defend against such attacks. Past research has shown [11] that OSINT can provide valuable support in this area. While it can be a valuable tool for detecting APT attacks, relying solely on OSINT is not sufficient. One of its weaknesses is that the data it provides may lack context, which makes it difficult to fully understand the motivations and goals of potential APT attackers.

To avoid relying solely on OSINT for detecting APT attacks, this study uses two prevalent models of cyberattacks: MITRE ATT&CK, and the cyber kill chain. MITRE ATT&CK is a matrix that contains a set of TTPs used by adversaries in each phase of their attack. The cyber kill chain, on the contrary, is a series of seven steps that describe the stages of an APT attack. We use these two models to correlate the attack-related behavior of an APT, from the reconnaissance phase to the attainment of its objective, with the TTPs used. This provides valuable insights into the objectives of the attack at an early stage, thus allowing for the detection of and response to potential APT attacks. For ease of use, the TTPs used in the technique of APT detection proposed here are referred to as "multi-stage attack-related behavior." We leverage both MITRE ATT&CK and the cyber kill chain to develop an effective method for the early detection of APT attacks that considers their attack-related behavior.

Our systematic literature review (SLR) begins with a summary of the relevant studies and their significance in the section "Related work." The section "Research methodology" outlines the methodology used to identify the research considered in this review. The section "Results of the review" provides a classification and explanation of all the methods of APT detection reviewed here based on the approaches taken by them. The section "Discussion" provides a critical analysis of strategies of APT detection by considering attack-related attributes from both academia and the industry. Finally, the section "Future works" summarizes the conclusions of this study and provides directions for future research in the area.

Related work

Several cybersecurity measures and methodologies are used to detect, monitor, and mitigate the effects of APTs. Yet, they continue to pose a daunting challenge to network security due to the use of sophisticated attack vectors, a multi-stage attack approach, and unknown vulnerabilities in the target networks. A multi-stage attack is a collection of steps taken by the attacker with a single defined goal within the network, and involves at least two activities that are part of the same attack scenario.

Researchers are interested in understanding how models of multi-stage attacks, like the cyber kill chain and MITRE ATT&CK, can be used to detect APTs from different perspectives. Examples include refs [10–16]. Tools of APT detection are being quickly adopted in the cybersecurity industry considering raising concerns over targeted attacks. According to Ahmed et al. [16], it is anticipated that the global sales of APT protection solutions will rise from $6.9 billion in 2022 to ~$15.2 billion by 2026. This underscores the industry's significant concern regarding the APT threat.

Although several studies have considered the multi-stage model of attack for APT detection, few researchers have conducted systematic reviews of work in the area. According to Robinson and Lowe [17], traditional literature reviews have such limitations as a lack of comprehensiveness, writer bias, and an inability to appropriately distinguish between methods of APT detection. Furthermore, prevalent reviews have neglected to provide a rigorous evaluation of commercially available technologies for APT detection. To fill this gap in the relevant research, we conduct an SLR of studies on APT detection based on a multi-stage model of attack in academia and the industry, and identify their strengths and weaknesses.

An SLR reviews research in a more methodical manner than a conventional literature review. Furthermore, according to Pahlevan et al. [18], the SLR can be used to categorize, select, and critically evaluate past findings. Techniques used for SLRs are established prior to the review process. It is a well-organized and thorough process that involves the assessment of numerous scholarly resources [19, 20]. This study makes the following contributions to research in the area:

(i) We explain prevalent techniques of APT detection as well as recent technological developments in the area in academia and the industry.
(ii) We detail technologies and methods of APT detection, and provide a critical summary of prevalent work in the area.

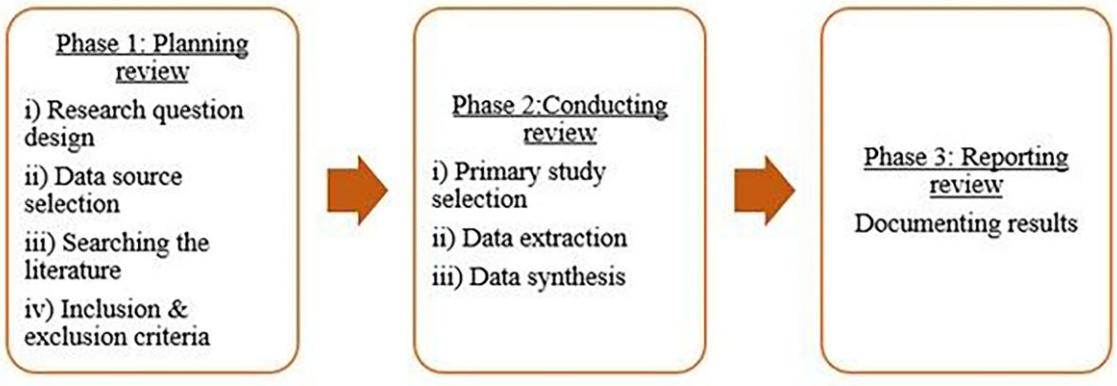

Figure 1. Phases of systematic literature review.

(iii) We examine issues in the area, and propose an improved method of APT detection based on attributes of such attacks.

A primary merit of this study is its use of the SLR for classifying and analyzing prevalent studies in the area. The aims are to (i) compile currently available commercial tools for APT detection and published research in the area in a structured manner, (ii) assess the relevant research, and (iii) prevent the omission of important work. This review is also guided by the research questions provided in the subsection "Formulation of research questions."

Research methodology

In terms of the research methodology, this study has opted for the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) approach to conduct an SLR. As a protocol-driven methodology, PRISMA is chosen to facilitate the identification of the most pertinent literature sources [21]. The selection of PRISMA as the review framework is underpinned by its inherent characteristics of transparency, accuracy, accessibility, and scope, which align well with the objectives of this research [22]. This investigation employs the methodological framework delineated within the extant literature, thereby ensuring a comprehensive analysis of the available research body [23]. Illustrated in Fig. 1, the procedural trajectory encompasses the following three principal phases: pre-review planning, review execution, and report articulation.

It is noteworthy that the design of the review process for this SLR was strategically formulated prior to the commencement of the study. The procedural outline encompassed several key steps, namely, (i) articulating the study's purpose, (ii) formulating a rigorous search strategy and precise selection criteria, (iii) devising an evaluative checklist for assessing study quality, and (iv) establishing a systematic protocol for data extraction. The adherence to the recommendations and guidelines proposed by Luh et al., Vaismoradi et al., and Braun and Clarke [24–26] served as a methodological compass, ensuring the research's robustness and comprehensive coverage.

Phase 1: planning the review

During the initial phase of the SLR process, the research questions are formulated to address the study's objectives. Additionally, the data sources, inclusion, and exclusion criteria are defined.

Formulation of research questions

A systematic review is founded upon a specific research question, established in accordance with the PICo framework (Problem, Interest, and Context). Building on these principles, the review encompasses three main aspects: APT attacks (Problem), detection techniques (Interest), and multi-stage attacks (Context). The following research questions (RQ) and objectives are devised through three analytical approaches:

(i) Trend Analysis answers RQ1: "What is the trend in APT detection techniques from January 2015 to April 2022?" This analysis seeks to illustrate the spectrum of methods employed in APT detection over the specified timeframe, spanning both academic and industry domains.
(ii) Strategy Analysis addresses RQ2: "How does an APT attack methodologically differ from other types of cyber-attacks?" This analysis aims to enhance understanding of distinctive attributes characterizing APT attacks and propose viable alternatives for enhancing detection techniques.
(iii) Behavioral Analysis responds to RQ3: "Which specific APT characteristics contribute to detection efficacy?" This analysis aims to uncover unique traits of APT based on previously reported instances and their potential to optimize detection rates.

Selection of data sources

The SLR encompasses data sources from both academic and industry domains. The chosen data sources include RSA Marketplace, Gartner Magic Quadrant, Radicati Market Quadrant, Google.com, ACM Digital Library, IEEE Explore, Springer, Elsevier, Scopus, and Wiley Online Library. The search string recommended by Julisch and Brogi [27, 28] is used to explore these sources. Selection of these sources is based on their relevance, impact, and quality of articles cited in this evaluation.

Literature and industry work search

The search process is conducted from two distinct perspectives, aligned with the primary objectives of this study, with a focus on academic research followed by industrial research. The search string is carefully crafted, incorporating pertinent keywords and their alternatives.

(i) Searching the literature

The exploration of academic research begins by scrutinizing article titles and abstracts. During this phase, a total of 90 articles were

excluded due to their focus on attack modeling rather than attack detection and concentration on single-stage detection rather than multi-stage detection. Ultimately, 35 articles were included. This stage also involves determining related synonyms, phrases, and keywords such as Advanced Persistent Threat, Advanced Persistent Threat detection techniques, multi-stage attack, MITRE ATT&CK, cyber-kill-chain, and tactics, techniques, and procedures (TTP). This broader approach enhances the potential for discovering relevant articles for the review, as recommended by Ghafir et al. [29]. Keywords tailored to the research questions are formulated, drawing from online thesauruses, previous studies' keywords, and database search engine suggestions. These keywords are then refined using Boolean operators, phrase searching, truncation, and wildcards.

(ii) Searching the industry work

The exploration of industry-related sources involves gathering and evaluating data from Gartner Magic Quadrant, Radicati Market Quadrant, RSA Marketplace, and Google.com to identify top cybersecurity and endpoint protection providers in 2022 (as indicated in Table 1). Keywords such as Advanced Persistent Threat, Advanced Threat, Zero-Day Threat, and Advanced Protection Threat are employed in these searches. The strategy aims to uncover relevant information from these selected resources. Specifically, 18 out of 36 service providers prominently offer solutions targeting the APT attack. Following these steps, the pertinent products from identified brands are closely examined to assess their features and functionalities.

Table 1. Provider of cyber-security and end-point solution.

No	Source	Provider	APT solution
1.	Radicati	Symantec/Broadcom	√
		ESET	√
		Cisco	√
		Bitdefender	√
		Kaspersky	√
		Sophos	√
		Trellix	√
		Palo Alto Networks	√
		VMware	√
		Microsoft	√
2.	Gartner	Trellix	√
		Symantec/Broadcom	√
		Microsoft	√
		Trend Micro	√
		Sophos	√
		Singularity Platform	X
		Falcon	X
		ESET	√
		Malwarebytes	√
		BlackBerry	X
		Cisco	X
		VMware	√
		Check Point	√
		Fortinet	√
		WatchGuard	X
		Open Text (Webroot)	X
		Cybereason	X
3.	Google.com	Microsoft	√
		Palo Alto	√
		Morphisec	X
		IRONSCALES	X
		Check Point	X
		FireEye	√
4.	RSA Marketplace	Threat X	X
		Secureworks	√
		AT&T Cybersecurity	X
		ExtraHop	X
		CyGlass	X
		Bitdefender	√
		Trellix	√
		Morphisec	X
		Securonix	X
		Tessian	X

The √ indicates the provider with APT solution.
The X indicates the provider with a non-APT solution.

Eligibility and exclusion criteria

SLRs are designed to systematically analyze and synthesize the existing research on a specific topic, within a defined time frame to identify gaps in the existing knowledge and inform future research. By limiting the time frame, SLRs can ensure that the most up-to-date and relevant research is included in the analysis. As a result, we define that the studies and industry work must be published within the defined period, which is January 2015 through April 2020. Taking studies before 2015 into consideration may not be suitable as the field of APT is constantly evolving and adapting to new technologies. APTs are known for utilizing the latest advancements in technology to penetrate networks, and therefore a more recent time frame is necessary to capture the latest developments in APT detection techniques.

Furthermore, to the best of our knowledge, within our specified time-frame, an APT detection technique based on multi-stage and vulnerabilities was not yet systematically reviewed. While previous surveys on APT detection methods [19–21] and multi-stage attacks [22] or both [23] have been conducted and published before our defined time-frame and in recent years, they differ in scope from our study. Our research advances the field by specifically examining the correlation between APT attributes and vulnerabilities in the network, offering a more comprehensive understanding of the issue.

For this study, a different time frame has been defined for industry work, covering the period from January 2022 to December 2022. This time frame has been selected to capture the most recent advancements and developments in the field of APT detection in the industry. The inclusion is different from that of academic research due to the rapid pace of technological advancements in the industry. The highly competitive nature of the cybersecurity industry drives companies to continuously innovate and develop new solutions, resulting in a faster pace of change in the field compared to academic research.

Other than that, only tools, journals, conferences, book chapters, and studies with related keywords have been included. The commercial tools and studies published before and after the specified duration were excluded. Studies other than the English language were not considered. Reports, magazines, and publications other than the journal, conference, proceeding, and book chapters were excluded. As to avoid any ambiguity or difficulty in translation, the search effort eliminated non-English publications and focused solely on English-language content. Tables 2 and 3, describes the inclusion and exclusion criteria for literature and industry work.

Quality assessment criteria

A quality assessment of selected commercial products and literature is required to ensure the validity of an SLR. The main goal was to include high-quality findings that linked to the research issue and to prevent biases in primary study selection. The approach facilitates researchers to find primary studies that are of high quality and able to answer the research questions. As a result, this study adheres to the methodology of Luh et al. [24].

Table 2. The eligibility criteria.

Criterion	Literature work	Industry work
Type	Journals, conferences, articles, book chapters, and studies related to defined keywords	White paper, reports, market research report, and product sheet related to APT solution
Timeline	January 2015 until April 2022	January 2015 until April 2022
Language	English	English

Table 3. The exclusion criteria.

Criterion	Literature work	Industry work
Type	Report, magazine, and publications other than the journal, conferences, proceeding, and book chapters	White papers, reports, market research reports, and product sheets not related to APT solution
Timeline	Earlier than January 2015	Earlier than January 2022
Language	Non-English	Non-English

The following are four QA (Quality Assessment) criteria that were used to assess the quality of primary studies:

(i) QA1: Does the study provide an answer to the SLR's research questions?
(ii) QA2: Does the study adequately describe the goals and methods of the study?
(iii) QA3: Does the objectives and results are clearly described?
(iv) QA4: Does the study contribute valuable addition to the relevant field?

All the selected primary studies were assessed based on the quality assessment criteria described above. The ordinal response scale has been used to evaluate the result where the scoring scale has been defined as, yes = 1, No = 0, or Partial = 0.5.

After applying the above QA criteria, it was discovered that 25 literature works did not meet the requirements, thus, these studies were excluded. The remaining 35 were taken into consideration to be the primary source for the study. While for industry work, 18 out of 36 do not match the criteria and are therefore not included in the analysis.

Phase 2: conducting the review

This section presents the activities of conducting the review based on the PRISMA framework, which involves primary study selection, quality assessment, and data synthesis.

Primary study selection

The PRISMA framework was used to identify, screen, eligibility, and inclusion criteria to include the most relevant information for this SLR, as shown in Figs 2 and 3.

For literature sources, as described in Fig. 2, during the first stage, the search technique and the search phrase were used to identify the related literature. Followed by screened stage, in which, out of 234 articles are eligible to be reviewed, a total of 180 articles were removed due to duplication and does not meet the inclusion criteria. The third stage is eligibility, where the full articles were accessed. After careful examination, a total of 25 articles were excluded as some did not focus on techniques to detect the APT or did not focus on the multi-stage attack behavior. The last stage of review resulted in a total of 35 articles that were used for the qualitative analysis (Fig. 2).

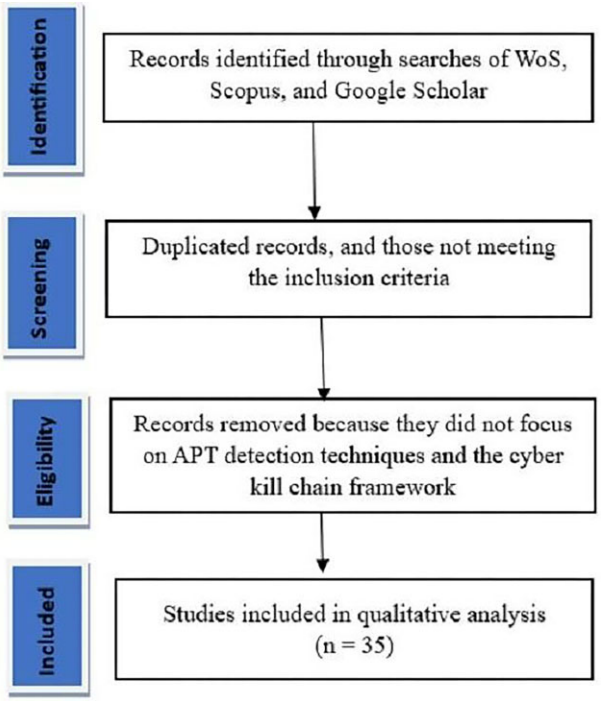

Figure 2. PRISMA framework for literature source.

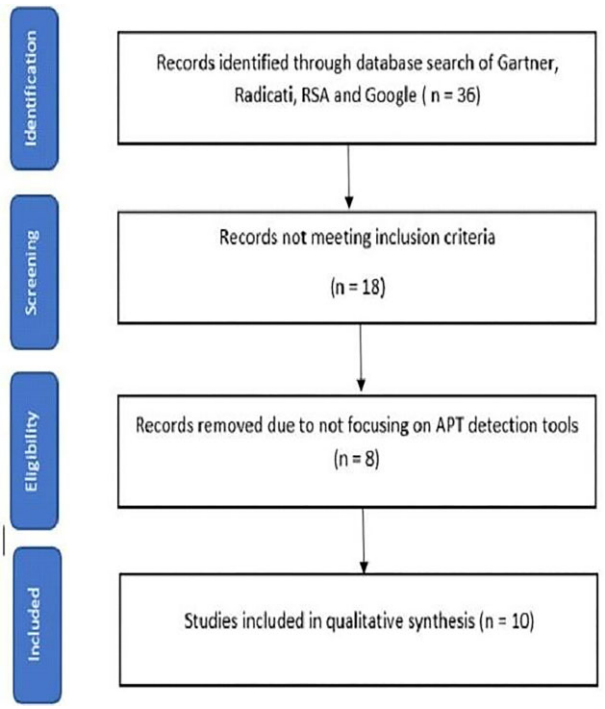

Figure 3. PRISMA framework for industry source.

While for industry sources, there are initially 36 companies that are related to the study's goal, as shown in Fig. 3. Then, 18 of them are excluded since they did not meet the requirements for inclusion. Later, in stage 3, eight of them were eliminated as a result of not concentrating on the APT detection technology. Only 10 of them, from the industry, are considered for further analysis at the final stage.

Quality assessment

For this SLR, a total of 45 papers were chosen to utilize the PRISMA framework, including 35 from literature sources and 10 from industry sources. The data extraction and quality assessment were performed in parallel.

Data synthesis

The data synthesis addresses the analysis in the SLR to summarize, interpret and integrate the review result. To accomplish the objective, 45 sources of information are read through, paying particular attention to the abstract, conclusions, and discussion sections for the scholarly sources and the product features and functionality for the industrial sources. Data abstraction was carried out based on the research questions, which means that whatever data from the examined studies could answer the research questions was abstracted and considered. Following that, a thematic analysis was conducted, which yield themes and sub-themes. Thematic analysis is defined as a descriptive strategy for flexibly reducing data and can be combined with other data analysis techniques [25]. Thus, the abstracted data were grouped and numbered to eliminate duplication, while also emphasizing linkages between the abstracted data [26].

Phase 3: reporting the review

The review's findings are examined, interpreted, and displayed thematically. The creation of topics is the initial step in thematic analysis. Patterns have been identified in the abstracted data of all reviewed sources during this approach. Any abstracted data that was comparable or related were grouped, resulting in a total of four main groups, namely the themes. A comprehensive discussion is provided in the following section.

Results of the review

We finally obtained 45 studies on methods of APT detection, and classified them into four themes based on the approaches used: (i) similarity-based methods, (ii) causal correlation-based methods, (iii) structural methods, and (iv) case-based methods. The distribution of the studies is shown in Fig. 4.

The approaches used by researchers to gather data and build technologies for APT detection form the basis for the classification shown in Fig. 4. It shows the techniques used to gather traces of attacks and their use to identify APTs. The evidence used in these studies to identify APT attacks includes packets, events, and alarms. We now summarize the contributions of each of the above-mentioned approaches/themes.

Theme 1: similarity-based methods of detection

This theme is based on the similarity among traces in the attack scenario constructed. We identified three further sub-themes: scenario grouping, progressive creation (through attribute matching or correlation), and anomaly identification.

Similarity-based methods of detection can construct attack scenarios based on the similarities between the steps of an attack. This is based on the idea that similar alerts have the same root cause [27], and thus are part of the same attack scenario. The main goal of such methods is to determine the degree of similarity between attacks. This makes them different from causal correlation-based methods, which focus on how a sequence of events is caused.

The similarity between traces of attacks is calculated based on one or more attributes or elements of each trace: IP addresses, port numbers, timestamps, or trace types. Each method of detection determines the measure to be used when comparing these different fields. It is usually written as a correlation index that can be binary (equal or not equal), or based on a more complicated correlation function. Similarity-based approaches have a major benefit over other methods in that they are easy to construct, and can return undiscovered multi-step attacks if the process used to determine the link between the traces is appropriately chosen. In general, a system for APT detection that uses these methods performs well because they compare only two sets of traces. However, the process of deciding whether the traces are related is complicated. If the strategy used to assess the correlation between traces is kept simple, and relies solely on the similarity among a few fields, the results yield an excessively large number of false-positive warnings. On the contrary, a sophisticated method of correlating traces of attacks, based on the application of correlation matrices and the use of various weights for each field, may be too particular to capture the characteristics of the entire spectrum of multi-step attacks. We divide similarity-based approaches into three sub-themes based on the way the degree of similarity is used to design attack scenarios: (i) progressive construction, (ii) scenario clustering, and (iii) anomaly detection.

(i) Progressive construction

Progressive construction is used to formulate the stages of an attack by adding similar traces to a scenario based on the similarity between them and other traces in it. The traces being compared are selected from the same temporal window, and are used to build sequences of traces sequentially and logically. The fields being compared may match exactly or partially. Exactly matching fields are known as (a) progressive construction with attribute matching, and partially matching fields are called (b) progressive construction with attribute correlation.

(a) Progressive construction with attribute matching

The authors of ref. [28] devised a strategy based on tags to discover the relationships between elementary attacks. Each step in a possible multi-step attack is assigned a tag, and the tags are spread throughout the system based on the flow of information. If two steps share features with coincident information, links between them are generated [29]. proposed a machine learning-based method of correlation between alerts that contains a detection module comprising eight strategies for identifying APTs. It encompasses all stages of a multi-stage attack as envisioned by the cyber kill chain model. The significant contribution of this study is its modeling of a technique of APT detection, namely, the MLAPT (Machine Learning-based Advanced Persistent Threat detection system) based on the correlation between alerts triggered by the detection module. However, some APTs may remain undetected owing to the limited number of techniques of detection considered in the study. In addition, the authors used human actions as the primary method for predicting APT attacks before applying the MLAPT module. This approach poses a high risk of generating false positives as human agents are prone to misinterpreting. Because APT attacks are dynamic and highly spe-

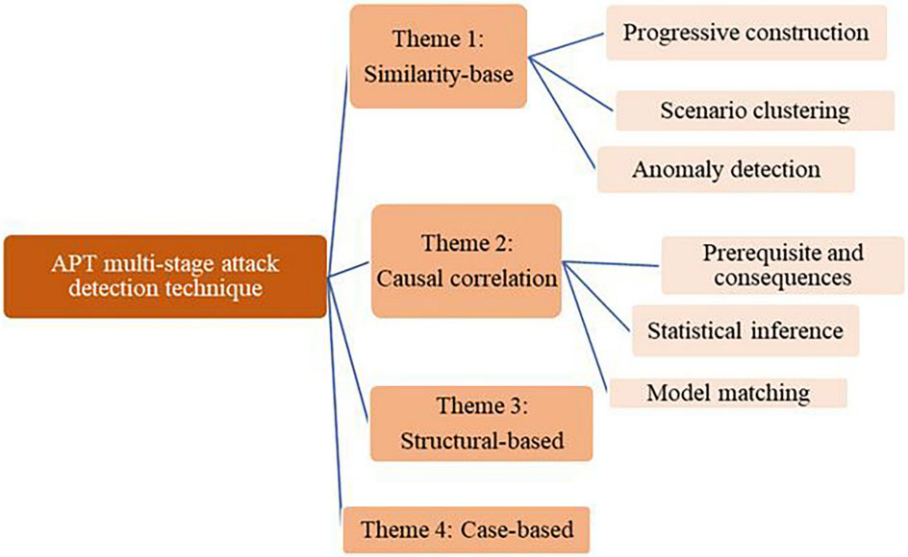

Figure 4. APT Attack in the Literature.

cific to the scenario at hand, the use of a scenario-specific attribute, as proposed here, may be more appropriate.

Furthermore, the authors of ref. [28] improved upon the work in ref. [29] by adding 14 detection modules. These modules were chosen based on a generalized method of APT attacks such that the approach proposed in ref. [29] is still applicable. However, the concerns highlighted by the authors of ref. [30] persist. The authors of ref. [31] proposed a model of the attack process that uses sensors to identify security-related and non-security-related incidents in constructing a chain of correlated alerts. "Security sensors" in this design refer to data from the IDS and anti-viruses, while "non-security sensors" refer to data retrieved from routers and Windows logs. A variety of sensors generate alerts over time, and are likely to detect an APT attack sequence. Identification is hence based on an analysis of causal relationships between consecutive stages of the attack chain. The results of experiments showed that this method can accurately rank hosts based on their likelihood of being infected by malware. However, this method requires a significant amount of computational power due to the variety of sensors used.

(b) Progressive construction with attribute correlation

The authors of ref. [32] proposed an approach that uses a correlation matrix, but distinguishes between the strengths of forward and backward correlations based on the temporal order of alerts. The authors of ref. [33] developed HERCULE, a system for "attack story reconstruction." They provided a long list of potential connections between events and used them to generate the corresponding graphs. Quadratic optimization was used to determine the weights associated with all edges in the graphs. The system outputs a comprehensive graph of all actions taken during a multi-step attack. The authors conducted simulations of their method by using several APTs from the literature. The three-layer ECorrelator [34] simulates the human immune system. It is built based on cells, which are vectors of the features of comparison including the similarity between IP addresses, and evolve through supervised learning from an initial set of fundamental principles. The strength of correlation between alerts is provided in each cell. The set of cells that are retained in memory form the foundation for the correlations identified.

Symantec's Advanced Threat Protection [35], developed by Broadcom, is a commercial software that integrates events at the endpoint, network, and email application, and correlates them through behavioral and file-based analyses. It uses a static method of detection to examine malicious files, which is effective for identifying disguised code. However, it cannot detect network vulnerabilities that compromise the security of an application at runtime.

The Sophos Intercept X Advanced with Endpoint Detection and Response (EDR) provides comprehensive protection against APTs through a four-pronged approach: prevention, detection, response, and investigation. It uses signature-based detection to identify known threats and behavioral analysis to detect unknown threats, and correlates event triggers based on the similarity in their attack-related behaviors. However, it fails to identify endpoint vulnerability, and cannot predict the node of the network that will be targeted. Moreover, it can detect and respond to a threat only on the node at which it was originally detected, which means that the threat is noticed only after it has already materialized.

VMware's Carbon Black Cloud uses the same approach as the Symantec software above, but with a focus on cloud-based protection. It can identify an APT by correlating trigger events, and provides administrators with valuable insights into the source of the attack and its intended target. However, it is effective only for endpoints with the agent installed, which renders unprotected endpoints vulnerable to attack. It is also limited to threats that occur on the endpoint itself, and cannot detect those originating outside it, such as threats within the network or the cloud. Like many security solutions, Carbon Black Cloud may generate false positives to trigger unnecessary alerts that require additional investigation, where this is time consuming and resource intensive.

(ii) Anomaly detection

Methods to identify APTs based on anomaly detection assess the similarity of incoming sequences of alerts against a set of non-malicious traces, and regard them as part of an attack if they deviate from normalcy. Abnormal behavior does not always correspond to an attack. Although techniques of anomaly detection have significant potential for generating false positives, they can also uncover previously unknown attacks.

The authors of ref. [36] proposed a method based on anomaly detection that randomly connects events from a training set that are free of attacks to generate certain hypotheses. They created a mathematical framework to describe the relevant theories, laws, and anomalies. Events that do not fit the theory are deemed abnormal, and trigger alarms. Because detection is performed on an event-by-event basis, the multi-step attack perspective is considered only during the characterization of a clean dataset. The authors of ref. [37] used hidden Markov models (HMMs) for anomaly detection. A clean dataset is used to construct a set of HMMs that reflect the sequences of typical occurrences. Sequences that do not match the learned models are abnormal, and to therefore represent a multi-step attack.

The authors of ref. [38] developed a scoring technique for detecting spear phishing emails by combining several criteria of anomalous behaviors. The technique differentiates between authentic and spam mail. Another common APT attack uses executable malware that can communicate with a botnet [39]. However, the use of a blacklist of IPs or URL addresses of botnets to defend against this attack is inefficient because it is always randomly generated. In light of this, the authors of ref. [40] proposed a method to mitigate the C&C channels of the APT. This approach involves identifying and detecting malware used in such attacks by observing patterns of anomalous behaviors of communication during web browsing. Analyzing anomalous behavior by traffic at the egress of the network is another prominent machine learning-based strategy to this end, and has been proposed by Adachi and Omote [41]. The authors of ref. [42] focused on the detection of lateral movements based on anomalies in malicious sessions of the remote desktop protocol (RDP) in Windows. Event logs are analyzed by using the RDP to monitor the delivery phase of the model of APT attacks. They used six machine learning algorithms to classify the sessions: logistic regression, Gaussian-NB, Bayes' theorem, the decision tree, the random forest, and logit boost. The results of experiments showed that the logit boost algorithm is the most effective for detecting anomalies in RDP sessions. However, not all types of exploits occur through the RDP in an APT attack scenario, because of which this method may miss traces of APTs. Like APT29, it uses the Kerberos ticket to initiate the attack. Because this solution is specifically designed for the RDP, it cannot confirm the presence of APTs owing to their dynamic mode of operation. Furthermore, its sole reliance on the lateral movement phase of the attack is inadequate because this does not prove that the captured movement is an APT. It can be improved if it can be configured to cover other stages, such as the exploitation phase, during which vulnerabilities are triggered in the victim network through specially crafted attack tools.

The authors of ref. [43] proposed the detection of APTs based on malicious features that are automatically selected and extracted from hidden layers of a neural network. They tested this method on the NSL-KDD dataset. The results showed that it is reasonably thorough as it can cover phases 1 through 6 of the CKC model of attack. However, it was able to extract only four classes of attacks from the given dataset: DoS, root-to-local (R2L) attack, user-to-root (U2R) attack, and probe attack. It is thus susceptible to false positives. The authors of ref. [44] proposed an attack model called strange behavior inspection (SBI) that is based on MITRE ATT&CK. It leverages anomalous behavior in the CPU, RAM, file registry, and file system. The model identifies the first potential victim of the APT based on credential-dumping techniques used by the attacker. The authors studied the process of APT identification by observing footsteps of the attack.

The authors of ref. [45] defined an APT attack as a five-stage process; delivery, exploitation, installation, command, control, and action. There are no defined means of transitioning from one phase to the next in this approach, and it can identify a variety of events in each stage that are then integrated. The scores assigned to each type of event are combined to obtain the result. Each host has an anomaly score, as does each cluster of the same type of events. APT attacks are defined as events with an anomaly score greater than a given threshold. The most significant disadvantage of this system is that it requires technical expertise for installation and maintenance.

The ESET Enterprise Inspector [46] is a powerful security solution designed to detect APT attacks. By leveraging advanced behavioral analysis and machine learning algorithms, it can identify patterns of suspicious activity that may indicate the presence of an APT. It monitors the endpoints of the network and the activity of the server in real time to correlate events across the environment, and can detect stealthy and multi-stage attack-related behavior associated with APTs. The solution identifies anomalies and potential IOCs, thus providing security teams with the information needed to investigate and respond to potential threats. However, as with any security solution, the ESET Enterprise Inspector is imperfect, and may generate false-positive alerts. Such alerts may require additional investigation and thus impact productivity. False positives can be particularly problematic in case of the ESET Enterprise Inspector due to its focus on behavioral analysis. Therefore, organizations using it should be prepared to address false positives as part of their overall security strategy.

Cisco Secure Endpoint's machine learning algorithms analyze large amounts of data to identify patterns and anomalies that may be indicative of APT-related activity. By examining endpoint activity across dimensions, including network activity, file behavior, and system calls, it can detect APTs that may have evaded traditional signature-based methods of detection. Some APTs use advanced techniques of evasion, such as fileless malware or rootkits, to evade detection by security solutions. While Cisco Secure Endpoint uses sandboxing and other techniques to detect these types of threats, they may not be completely effective. It may also not be able to detect zero-day attacks. These are attacks that are not yet known or documented, which makes them difficult to detect by using signature-based techniques or even behavioral analyses.

(iii) Scenario clustering

A scenario clustering-based approach applies a clustering algorithm to the entire collection of alerts and returns certain clusters as potential scenarios without considering their order, as in the case of progressive construction. Clustering aims to identify naturally occurring groups in a given dataset [47], Automatic clustering algorithms are typically used to this end. These groupings or clusters are then regarded as potential multi-stage attacks. A high degree of similarity between traces from the same scenario is required when comparing traces from different scenarios.

The authors of ref. [48] proposed a method for clustering IP addresses based on a particular parameter. They made an original contribution by using notifications from a web application firewall (WAF). The high degree of abstraction used by the WAF makes it possible to understand the attacker's intentions. A method for the hierarchical clustering of networks that reflects attack-related strategies was proposed by Kawakani et al. [49]. Graphs are automatically generated from alerts in the same time window by matching the attributes of IP addresses. Once the clusters have been built, they can be applied to the classification of new scenarios.

The authors of ref. [50] focused on detecting APTs in a cloud environment based on their semantics. They developed code to detect APT attacks based on attack-related behavior throughout the

operation of APTs on the target system. Following this, they created rules for inferring attacks based on the observed behavior. However, its dependence on rules-based detection may limit its success as such regulations must be continually updated to keep up with the dynamic behavior of APT attacks.

The authors of ref. [51] proposed APTMalInsight, a framework for detecting APTs, by leveraging system call information and a semantic ontology. This approach can be perceived as phase 3 of the CKC attack model: the delivery phase. The authors used the semantic ontology to construct the behavioral framework of APTs through event analysis of the network. Following this, they examined the APTs and clustered them into families. However, they were not able to automatically build the foundation for semantic ontological knowledge as they had intended. Instead, it was implemented manually, whereby a list of pre-defined APT behaviors was matched with the attack-related data. This information needs to be frequently updated to avoid confusion. Reliance on a list of behaviors for detecting an APT is inadequate because the behaviors hence described are comparable to those of other cyberattacks, and are not recognizable only as related to an APT attack. Combining this approach with different phases of the CKC model of attack, such as phase 3 (the exploitation phase), may yield a more accurate confirmation of the presence of APTs.

Theme 2: causal correlation-based methods

The architecture of multi-stage attacks and the causal relationship between its steps are the main issues considered for the detection of APTs in this set of techniques. We identified three sub-themes: prerequisites and consequences, statistical inference, and model matching. The key to determining how a multi-step attack occurs in the context of methods based on causal correlation is to identify how the sequences of traces lead to one another. In other words, decisions made earlier influence those made later, and a causal chain can be formed due to this link.

Lu et al. [52] emphasize the nature of multi-stage attacks as sequences of stages, which is the most reasonable interpretation of these threats that is currently available. Their adaptability allows for the discovery of small variants of known attacks but not entirely new ones. False positives may still occur, but are likely to be fewer than are obtained in approaches based on similarity along with the use of hypotheses. The three sub-themes are as follows: (i) prerequisites and consequences; (ii) statistical inference; and (iii) model matching.

(i) Prerequisites and consequences

In these approaches, each alert is expected to contain a set of prerequisites, also known as preconditions, and outcomes, or post-conditions. The circumstances that must be satisfied for an attack to be effective are known as the prerequisites, while the probable results of the attack are known as its consequences. The multi-stage attack recognition system (MARS) is the most comprehensive method of detecting multi-step attacks based on prerequisites and consequences [53].

(ii) Statistical inference

Statistical inference is the process of determining the distribution of a dataset from the data themselves [54]. It operates under the assumption that the required information is already present in the dataset of traces, and all that is required of us is knowledge of where to look for it. A probabilistic model that can be used to detect attacks is constructed by using such statistics. Bayesian inference is perhaps the most widely used technique of statistical inference, both in general and for detecting multi-step attacks. HMMs are also commonly used to visualize the findings of statistical inference. The authors of ref. [55] proposed using a rapid fuzzy clustering algorithm to categorize alerts that is based on the similarity between IP addresses, ports, and timestamps. The given dataset is mined while considering only the type of alert as a feature. HMMs have also been used to detect multi-step attacks via statistical inference. They make use of IDS alerts that have been categorized beforehand into groups that correspond to each of the typical stages of a complicated attack. An HMM must be specific about how its steps are connected, and IP addresses are used to this end.

(iii) Model matching

Methods of model matching differ from case-based methods in that the latter employ the characteristics of actual attacks. Model matching-based approaches represent the skeleton and general aspects of a multi-step attack at a high degree of abstraction. Past research has suggested that the model of the global phases of the APT can be used to derive a feasible model for its detection [56]. The structure of such a model should consist of a series of sequentially ordered phases, one for each step of the attack. Traces that have previously been connected to a phase can be compared to the model and linked based on similarity.

Theme 3: structural methods

Such techniques of detection are based on attack traces that are projected onto a model of the network. Numerous techniques of intrusion detection consider the topology of the network to be crucial, and use information, particularly data on vulnerabilities affecting each asset, for attack identification. This information is structural in that it depends solely on the system being protected, and not on the actions of the attacker. The latter are inferred from the former, although no true trace-based evidence is used.

The authors of ref. [57] proposed using attack trees from a graphical model of security as a common language to systematically depict intricate multi-stage attack scenarios in a way that is user friendly. They simulated three well-known APT attacks: Stuxnet, Black Energy, and Triton. The results showed that the attack tree-based model could visualize complicated attack scenarios. However, an attack tree can grow and become complicated in case of certain attacks. There may be hundreds or even thousands of distinct routes to the successful conclusion of an attack. This significantly complicates troubleshooting for the network administrator.

The authors of ref. [58] proposed DeepAG, a framework that makes use of system logs to identify risks and predict attack vectors. DeepAG uses transformer models to represent semantic data in the system logs to identify APT attack sequences. It uses bidirectional prediction for attack pathways by using an LSTM network, which outperforms the typical BiLSTM in terms of performance. Attack graphs that attackers might use to breach the network are created by DeepAG as well. Although it outperforms competing software, it struggles to close the semantic gap between different kinds of logs. Based on a dynamic attack graph and evolution of the network [59], proposed the targeted complex attack network to identify the process of the APT attack. The primary objective was to identify hosts that were unquestionably involved in the attack process. The authors identified suspicious hosts linked to APT-related activities by using social engineering and network penetration. However, this method cannot determine the entire path of attack in case of node failure during the attack.

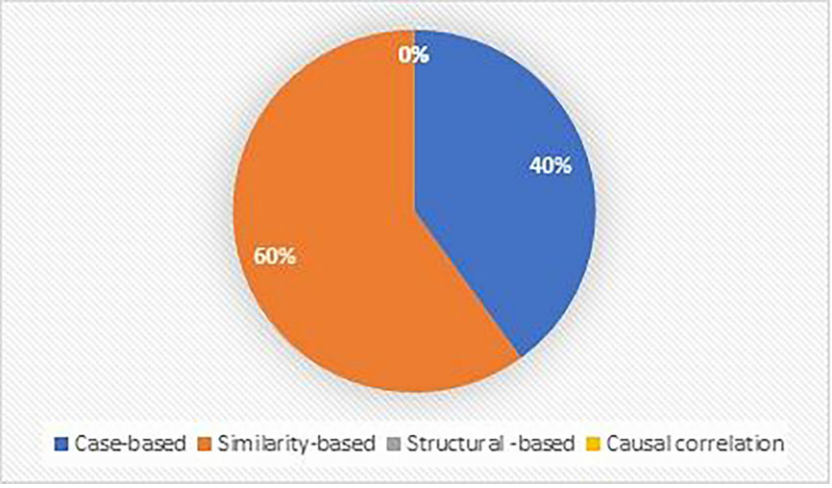

Figure 5. Adoption of APT detection techniques in Scholar's domain.

Theme 4: case-based methods

Comparing observations of attack-related behavior in a network with a knowledge base of previously observed attacks is a widely used technique for intrusion detection. There are numerous ways to implement this strategy in case of multi-step attacks. Scenarios or sets of actions are used to depict attacks in this case. Security experts can manually add attacks to the knowledge base or automatically extract them from a dataset.

The authors of ref. [60] proposed a system to detect APT attacks based on the behavior of the DNS. This approach corresponds to phase 6 of the CKC attack model. However, in contrast to the method proposed in ref. [29]. that relies on log files, this is a real-time technique to monitor DNS traffic. The authors defined relationships between the DNS request message and the DNS response as an attribute for identifying APT attacks. Nevertheless, because the detection system runs on the same DNS server as the malicious domain name, some legitimate DNS traffic is flagged as suspect by the algorithm. The authors of ref. [61] proposed detecting APTs by analyzing DNS logs and network traffic through a signature-based and anomaly-based detection technology. They established 14 characteristics of the DNS to detect traffic from infected clients that are managed remotely, and combined various feature vectors to create a reputation engine that determines if an IP address is compromised. However, a weakness of this strategy is that it does not work well when an attack does not involve domains, such as when a Trojan infects the computer by resolving an IP address to connect to a C&C server.

Two commercially available tools that apply case-based methods: Kaspersky's Anti-targeted Attack Platform [62], and Bitdefender's Gravity Zone [63]. Both use a combination of advanced technologies and threat intelligence to analyze malicious behaviors and form attack scenarios. However, both tools occasionally yield false positives owing to their heavy reliance on the use of a signature-based detection system and sandboxing as a first line of defense. These methods are also ineffective in detecting attacks that require user interaction to be activated, like phishing attacks. APTs are known for their stealth, which makes it difficult to detect them by using this approach. Even if machine learning techniques are applied subsequently in the process, they are likely to be ineffective owing to the inaccurate first-tier data.

Advanced Threat Defense (ATD) and Wildfire are two powerful tools designed to detect and respond to advanced threats, including APTs. ATD is a tool to detect APTs developed by Trellix, while Wildfire is offered by Palo Alto. A key benefit of these tools is their close integration with security solutions, including those for network and endpoint security. This allows them to analyze and correlate network traffic to form a detailed attack scenario. In addition, both tools rely on IOCs to detect and correct threat infiltration. It is important to note that APTs use dynamic attack code, where this makes it difficult for traditional techniques of sandboxing and static code analysis to detect them. However, ATD and Wildfire use advanced behavioral analysis and machine learning algorithms to identify and respond to APTs. A limitation of these tools is that they lack an email gateway solution, which means that they may not be able to detect the initial stages of an APT attack, such as phishing emails, and malicious attachments or URLs. Overall, ATD and Wildfire are highly effective tools for detecting and responding to APTs, but organizations should consider additional security measures, such as email security solutions, to fully protect against such attacks.

Discussion

This SLR analyzed techniques of APT detection based on multi-stage attack-related behavior. The latter is identified based on the TTPs used by the APT during the attack. Five themes were identified to investigate how researchers constructed their system of detection by using attack events. The results of an analysis of each of the themes are provided below.

Classification-based analysis

Classification-based analysis is used to examine the patterns and distribution of research on techniques of APT detection, as well as the factors that impact academia and the industry in their choice of techniques. We used thematic analysis to identify, analyze, and interpret patterns of interest in techniques of APT detection. Thematic analysis, as defined in ref. [26], is a means of analyzing qualitative data that involves searching over a collection to identify, analyze, and report on repeating patterns. We used it to identify the four themes shown in Fig. 4. They highlight the strategies used to accumulate traces of APTs and develop tools for their detection. For ease of interpretation, Figs 5 and 6 show statistical perspectives of both academia and the industry for identifying patterns of techniques of APT detection proposed in the 45 studies considered in this review.

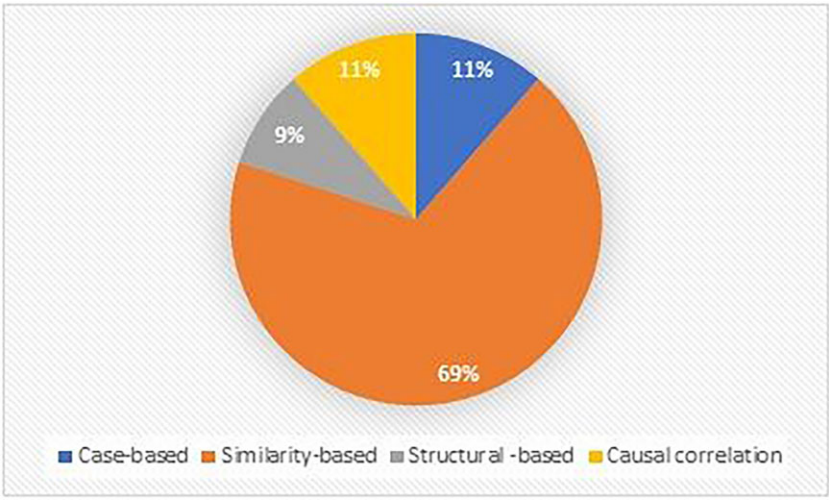

Figure 6. Adoption of APT detection techniques in the industry domain.

Figures 5 and 6 show four distinct techniques that have been used in academia and the industry to find traces of APTs in the 45 studies considered here. Only similarity-based techniques have been frequently used by both, with a rate of use of 60% in the industry and 69% in academia. This method is predicated on the notion that related traces are indicative of the same APT-related scenario, and this can be demonstrated by establishing correlations with a widely used architecture for an APT attack, such as the cyber kill chain and the MITRE ATT&CK. This helps show that the APT being tracked is real, because of which this class of methods is popular among both academics and industry experts. The term "traces" refers to alerts and events generated by network security applications. The authors of ref. [29]. conducted a similarity analysis of an alert produced by an IDS to determine whether the relevant traces were associated with an APT based on the IP address, port number, and alert type. They used the framework of the cyber kill chain, which can represent an attack sequence, to this end. Even though its implementation appears straightforward, determining how the traces are linked to one another is a difficult task. If the method used to connect traces considers only similarities between a small number of fields, the outcome may include numerous false-positive alarms. Moreover, a false negative can occur if the connection formed is too complicated and involves the use of different weights.

The case-based approach was the least popular choice for detecting APTs in academia, with a rate of use of only 11%. It involves manually generating models of attacks by using a knowledge base of past attacks. As it is simpler to locate the precise occurrence of the search word from the available knowledge base, implementing such approaches has the distinct advantage of lowering the number of false positives. However, this technique can be used only to find a known APT attack, and cannot identify patterns of attacks that are absent from the database used.

The structural and causal correlation-based techniques were the least commonly used in the industry. Structural methods are also known as white-box techniques, and require that the internal structure of the network be known beforehand. The informational structures of the nodes include details on the hardware and software used as well as any vulnerabilities that may be present. APT traces are forecasted based on these data. The industry is not particularly interested in this technique because it integrates such components as asset-related information, network topology, and vulnerability-related information, which together comprise at least three independent systems but must be combined to provide real-time data. The company thus incurs considerable overhead when implementing it. Moreover, it is difficult to integrate third-party technologies if an organization already has an internally compatible asset management system. By contrast, causal correlation is a method for finding APT traces that depends on knowledge of earlier events. Techniques must be "aware" of the types of privilege obtained and the vulnerabilities that have been exploited. This method differs slightly from the structural method of APT detection because it does not require node-related information. Instead, the exploited vulnerability and privilege gained are used as a guide to identify the APT.

The findings of our analysis show that exploiting vulnerabilities is the only way in which an APT attack can be successful. Therefore, APT detection that incorporates vulnerability identification is more effective than otherwise. This strategy has the potential to develop excellent APT detectors, but requires better means of using attack-related data. Data related to APT attacks or traces of vulnerability in the network architecture should be used to better understand attack-related behaviors and the likely course of attacks. APT traces, for instance, include IP addresses and port numbers that can be used to identify the infected network devices. Vulnerabilities can be discovered once the affected host or system has been located. Based on the identified weakness, predictions can be made about what the APT might do next to progress. Thus, APTs can be identified at the earliest possible stage.

The above classification-based analysis suggests that APT detection is mainly dependent on two elements: (i) the traces of attacks, and (ii) multi-stage attack scenarios. Traces can occur in the form of alerts generated by security devices, like the IDS and firewalls, and contains the IP address and port number of the initial target of the attacker. Furthermore, our analysis showed that researchers apply certain processes to ensure that the attack consists of multiple stage, regardless of the method of detection used. This is important because APT attacks always consist of multiple steps.

Strategy analysis

We now apply strategy-based analysis to analyze the findings of our SLR. The aim is to obtain a better understanding of how APTs are carried out to propose improvement to techniques for their detection.

Past works [64–66] have shown that APT attacks use a multi-stage approach. Each attack consists of at least two discrete actions performed by one or more attackers to accomplish a single aim within the network. If the two discrete attacks are comparable, the attack cannot be classified as a multi-stage one. For instance, millions of packets can be detected in case of a DDoS attack, but each constitutes a specification of the same type of action. We thus classify them as multi-agent single-step attacks. The attack-related behavior in case of the APT consists of multiple stages owing to the various TTPs used.

Companies such as Lockheed Martin, Dell, and BSI have developed a variety of models of attack, as listed in Table 4. Understanding them can allow security experts to better understand how an attacker might carry out an attack, which, in turn, can help them determine the appropriate protective measures to take for their organization. The attack model developed by Lockheed Martin is a patented cyber kill chain model that is commonly used in the industry to represent the various stages of an APT attack. Table 4 shows that the cyber kill chain consists of an attack cycle of seven steps describing the attackers' strategy for achieving their objectives. The model is the primary inspiration for other attack models, including SDAPT, Dell, LogRhythm, Mandiant, Lancaster, and BSI. They have a cycle of attack comparable to that of the cyber kill chain, with only slight variations in the titles and the number of phases. They are based on the same conceptual idea, and can be divided into three parts. The first part, which generally covers the first two or three phases of the attack, considers the attacker's actions that enable it to gain a foothold in the organization's network. The second section details the steps necessary to gain remote access to the company's network. The attacker's ultimate goals, such as data theft or system disruption, are addressed in the third part, which often occurs in the final two phases. These attack models focus on the phases that attackers must go through to reach their objective. Even though an attack may not explicitly follow all the phases of the attack model, the latter can serve as a useful reference. Understanding the stages of an attack is essential as it enables us to predict the attackers' goals and next moves. In addition, it is possible to demonstrate that the attack is an APT by comparing its traces with a probable phase of the model.

The phases of each attack model presented in Table 4 reflect the attacker's actions or methods for entry into the network, such as weaponization, targeting, or installation. The models also emphasize the attacker's objectives associated with each phase, such as reconnaissance and actions. However, they may be invalidated if unanticipated actions are carried out, or the order in which the actions are performed is disrupted. Attackers may not always follow well-known techniques, such as using C&C to monitor their attacks. For instance, the APT Stuxnet can autonomously carry out specific activities without needing to communicate through the C&C server. Therefore, an attack model that focuses solely on the activities and objectives of the attackers is insufficient for developing a successful technique of APT detection. As vulnerabilities are often a prerequisite for the success of an APT attack, the model must include a phase of vulnerability exploitation, in which the APT gains a foothold in the target network and performs internal reconnaissance to identify vulnerabilities that can be exploited. Once the vulnerabilities have been discovered, the attacker can escalate its privileges or retrieve information for lateral movement toward its objective.

Behavior analysis

Merely correlating the traces and phases of an attack is not sufficient to ensure an efficient technique of APT detection as it does not account for the attacker's operational understanding. We thus analyze APT attack-related behaviors to determine their unique intentions in conducting such attacks because this will make it easier to distinguish between attacks that originate from APTs and those from other types of threats. Our SLR showed that an APT uses a different attack vector that comprises TTPs tailored to the environment of the target network. Despite this, the TTPs share enough similarities to be grouped together for a simpler understanding, as is depicted in the data for MITRE ATT&CK in Table 5. MITRE ATT&CK was used to represent the TTPs of APTs because it provides extensive knowledge of the tactics and techniques of adversaries based on real-world observations. The ATT&CK knowledge base has been widely used as a foundation for the development of specialized threat models and techniques in the business, government, and cybersecurity sectors around the world. The CKC model, listed in Table 5, was chosen from among the attack models shown in Table 4 because it has been used in the industry for a long time. It is also a pioneering model in representing APT attacks as a multi-stage process.

We formulated Table 5 to gain deeper insights into the progression of APT attacks. By using the cyber kill chain framework and leveraging the TTPs outlined in the framework of MITRE ATT&CK, Table 5 serves as a comprehensive visual representation of such attacks. Its primary objective is to clarify the intricate stages of APT attacks to facilitate a comprehensive understanding of the patterns of attack and their interconnections. For example, APT 1 and APT 3 share the same TTPs, spear phishing emails, in the reconnaissance phase of their attacks [15]. The TTPs can be used to generate a threat profile that includes a complete description of a particular APT attack [67]. This profile also shows that an APT attack is executed in stages. As a result, an effective detection technique should be capable of correlating the traces, stages, and TTPs of attacks with the vulnerabilities of the network. Our analysis of APT attacks showed that attackers use a staged approach by using specific TTPs, such as spear phishing, C&C, and privilege escalation in each stage. We use the insights obtained from our findings to formulate Table 6 (Appendix A) in order to assess the extent to which current techniques of APT detection align with the imperative of detecting distinctive APT attack-related behavior. Such behavior encompasses multi-stage attacks, the use of TTPs, and the exploitation of vulnerabilities.

Table 6 (Appendix A) serves as a comprehensive mechanism to determine whether prevalent methods of APT detection can adequately defend networks against such attacks. By assessing the techniques of detection against the criteria for identifying and mitigating the intricate patterns of APT attacks, we aim to provide a comprehensive understanding of the strengths and limitations of current techniques of detection.

Our analysis highlights the significance of the multi-stage nature of APT attacks and their exploitation of network vulnerabilities. We thus recommend that these factors be considered as critical elements in the development of techniques of APT detection. The source of vulnerability-related data may be a database of known vulnerabilities, a scan of the network, or information on the context of the network. The ability to identify vulnerabilities is critical for security experts to proactively patch them before they can be exploited by an APT. However, it is also essential to consider the process of identifying the pertinent vulnerabilities because their sheer number in a network can make it impossible to address all of them. Establishing a correlation between the IP addresses, attack traces, and types of alerts is critical for understanding the pattern of the attack. This information can provide valuable insights into the attacker's movements within the network, and can enable security experts to take appropriate actions to prevent the attack. The attacker's predicted movement can be visualized by using an attack graph.

Table 4. APT Attack model in the literature [1–4].

APT attack model	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6	Phase 7	Phase 8	Phase 9	Phase 10	Phase 11	Phase 12
Cyber Kill Chain (2011)	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control	Actions on objective					
System for Detecting APT—SDAPT (2012)	External recon	Gaining access	Internal recon.	Expanding access	Gathering information	Extracting information	Control of information leaks	Phase 8: Erasing track				
Dell SecureWorks (2012)	Preparation	Initial compromise	Expansion	Persistence	Search and exfiltration	Clean up						
LogRhythm Model (2013)	Reconnaissance	Compromise	Maintaining access	Lateral movement	Data exfiltration							
Mandiant (2013)	Initial reconnaissance	Initial compromise	Establish foothold	Escalate privilege	Internal reconnaissance	Move laterally	Maintain presence	Complete mission				
MITRE ATT&CK (2013)	Initial access	Execution	Persistence	Privilege escalation	Défense evasion	Credential access	Discovery	Lateral movement	Collection	C&C	Exfiltration	Impact analysis
Lancaster Model (2014)	Recon., attack staging and initial host infection	Network intrusion, remote control, lateral movement, data discovery, persistence	Staging server selection, data preparation and data exfiltration									
BSI Model (2015)	Observer victim	Prepare/ Distracting attack	Final infection	Observe network	Gain privileges	Spy data/ sabotage of system	Continuous observation	Cover track				

Table 5. APT attack with respective cyber kill chain attack stages and MITRE ATT&CK tactic, technique, and procedures.

No.	APT attack	Multi-stage attack										
		Reconnaissance	Weaponization		Delivery			Exploitation		Installation	Command and control	Action on objectives
		Social engineering	Host-based	Network-based	Spear phishing	Watering hole	Rogue Software	0-day	known	Modify registry key	Https(s)	Data exfiltration
1.	APT 1	√	√		√	√	√	√		√	√	√
2.	APT 3	√	√	√	√	√		√	√	√	√	√
3.	APT 12	√	√		√			√	√	√	√	√
4.	APT 15	√	√		√			√	√	√	√	√
5.	APT 16	√	√		√	√		√	√	√	√	√
6.	APT 17	√	√	√	√	√		√	√	√	√	√
7.	APT 28	√	√	√	√	√	√	√	√	√	√	√
8.	APT 29	√	√	√	√	√	√	√		√	√	√
9.	APT 30	√	√		√				√	√	√	√
10.	Copy Kitten	√	√		√	√			√	√	√	√
11.	Molerats	√	√	√	√	√			√	√	√	√
12.	Silent Cholima	√	√		√			√		√	√	√
13.	Emissary Panda	√	√		√	√			√	√	√	√
14.	Olympic Game	√	√		√	√	√	√	√	√	√	√
15.	Energetic Bear	√	√	√	√			√	√	√	√	√
16.	Lotus Blossom	√	√		√	√		√	√	√	√	√
17.	Desert Falcon	√	√		√				√	√	√	√
18.	Snake	√		√	√	√	√	√	√	√	√	√

To be able to detect APT attacks early on, we incorporate their attributes into prevalent techniques for their detection. They include their multi-stage nature, vulnerability exploitation, and an attack graph, as illustrated in Fig. 7. Given the increasing sophistication of APT attacks, it is crucial that security experts use enhanced techniques, such as our guidelines, to detect and prevent these threats at an early stage.

Methods like ours have been proposed in the industry, such as security orchestration, automation, and response (SOAR), and risk-driven tools for vulnerability management. SOAR platforms typically provide a centralized console for managing security events and alerts from various sources, and prioritize threats for analysis and response. Risk-driven tools for vulnerability management, on the contrary, prioritize security vulnerabilities based on the risk that they pose to the organization. Our approach builds on the strengths of both tools but with a specific focus on APT attacks. While SOAR and risk-driven tools for vulnerability management are generic solutions to threat management, our approach is tailored specifically to detect APT attacks considering their multi-stage nature and vulnerability exploitation.

Academic research in the area has also led to the proposal of a method like ours: the topological vulnerability analysis (TVA) tool developed by Husari et al. [67]. This tool predicts known exploit sequences that attackers may use to compromise computer networks as well as correlated alerts to predict upcoming exploits. However, TVA is a broad strategy against attacks that occur in stages, and does not specifically target APT attacks. Its creators have not defined multi-step attacks in the context of TVA to match the typical APT, where this is addressed in our approach. Our approach is based on the cyber kill chain, a typical pattern of a multi-step APT attack that is included in our solution. The TVA tool generates many attack paths that can be difficult to comprehend and prioritize for administrators. The attack graph is generated by correlating attack-related alerts with network vulnerabilities, where this may generate numerous potential pathways for the attack. To defend more quickly against such attacks, it is important to plot the attack graph based on the likelihood of each node being exploited. Therefore, our approach enhances the TVA tool by providing a more focused and tailored solution for APT attacks.

Based on the gaps identified in this review, we have proposed an improved technique for APT detection, as shown in Fig. 7. It consists of four following modules: (1) alert identification, (2) alert correlation, (3) assessment of the vulnerability of the network to APTs, and (4) a probabilistic APT attack graph.

As shown in Fig. 7, the network traffic is scanned and processed to identify a possible attack or suspicious event according to the lifecycle of the APT. The technique of attack is based on TTPs from the MITRE ATT&CK framework. The alerts generated due to the detection of the TTP are then fed into the alert correlation module, the objective of which is to identify alerts that might be related to each other and a single APT attack. The notifications are filtered in this case to eliminated redundant alerts. Following this, the alerts for the same APT attack are grouped together. The APT attack scenario is compared against the database of assets and vulnerabilities in Module 3. A probabilistic APT attack graph is then generated in Module 4. The likelihood that each node will be exploited is determined in this stage, and the attack graph highlights nodes in increasing order of likelihood. By identifying nodes with a high likelihood of being exploited, this strategy reduces the complexity of the attack graph.

Future works

In our envisioned future research endeavors, we are committed to delve into the integration of AI methodologies with our proposed solution. AI technologies offer the distinctive advantage of real-time monitoring and swift response to potential threats, elevating the speed and efficiency of threat detection. Prominent examples like Vectra AI and Darktrace exemplify the prowess of AI-driven approaches in identifying APTs. By harnessing advanced artificial intelligence and machine learning techniques, these solutions dissect network traffic and behavioral patterns in real time, effectively pinpointing anomalies, and potential indicators of APT activities.

Vectra AI and Darktrace rely on an intricate web of behavioral analytics, anomaly detection, and AI-powered algorithms to scrutinize network operations. Their ability to identify deviations from established norms and flag suspicious activities mirrors our pursuit of unveiling latent attack patterns. These AI systems diligently absorb the baseline behaviors of networks and devices, enabling them to uncover nuanced and intricate attack strategies that might otherwise remain concealed.

Our proposed solution, hinging on the identification and utilization of system and network vulnerabilities, harmonizes seamlessly with the AI-driven paradigm. This is underscored by the symbiotic relationship between AI's capacity to detect anomalous behavior and active threats, and the pivotal role vulnerabilities play in furnishing the necessary context to prevent and mitigate potential cyber-attacks. This synergy emboldens our approach with a comprehensive security stance that addresses both proactive threat detection and the strategic management of system weaknesses.

Key highlights of integrating our APT Attribute-Vulnerability-based detection approach with AI methodologies include:

(i) The AI-approach excel at identifying ongoing attacks and unusual activities but knowing system's vulnerabilities allows us to proactively address potential entry points for attackers. By identifying and patching vulnerabilities before they are exploited, we can significantly reduce the attack surface and minimize the risk of successful breaches.
(ii) Vulnerabilities provide attackers with an initial foothold to infiltrate a network. By addressing vulnerabilities, we can reduce the likelihood of attackers gaining access in the first place, which complements the detection capabilities of AI-approach.
(iii) Not all threats can be identified solely through behavioral analysis. Zero-day vulnerabilities and novel attack techniques might not trigger behavioral alarms immediately. Knowing our system's vulnerabilities enables us to have a broader perspective on potential threats and take action to prevent them.

Therefore, incorporating AI-based approach like Vectra AI, Darktrace, and other advanced threat detection solutions alongside vulnerability management creates a comprehensive security strategy. It combines threat detection and response with proactive measures to reduce the likelihood of successful attacks, making your overall security posture stronger and more resilient.

Conclusion

This paper presents an SLR conducted between January 2015 and April 2022, focusing on the behavior of APTs during targeted, multi-stage, and covert attacks. The SLR encompasses a broad range of resources relevant to both the business and academic domains, providing a comprehensive overview of the current state of research in the field. The SLR process involved formulating research ques-

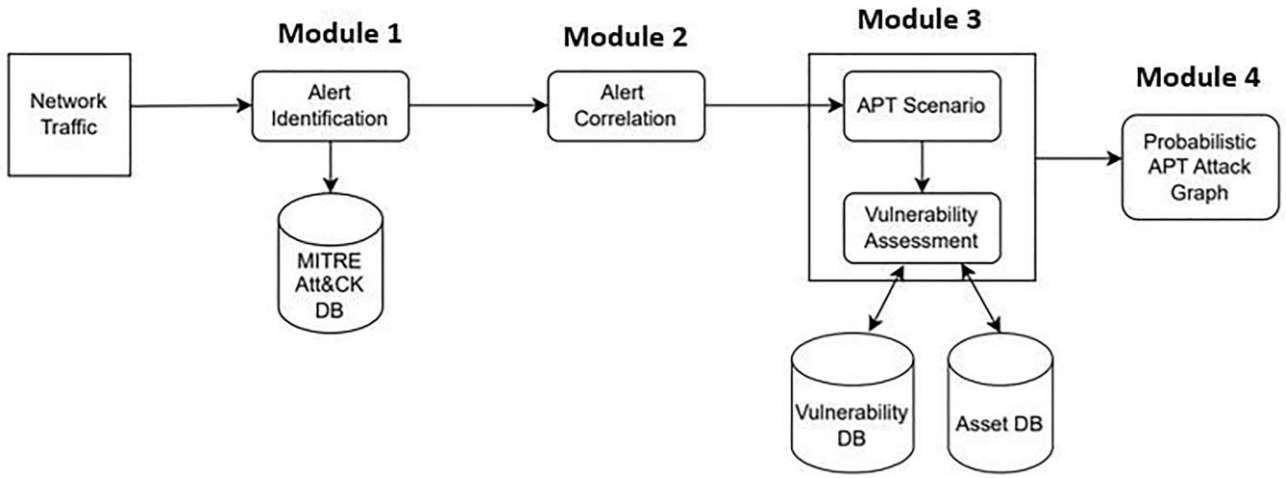

Figure 7. APT detection technique.

tions, employing a keyword search approach, and utilizing a recursive search method guided by predetermined inclusion and exclusion criteria.

From the collected literature, four key themes pertaining to detection strategies for APT attack behavior were identified. Specifically, the selection criteria prioritized papers that emphasized multi-stage attacks. Additionally, the chosen resources were examined in relation to another crucial attribute of APT attacks: TTPs, as well as their stealthy nature.

However, the SLR findings revealed a lack of resources that investigate the correlation between vulnerabilities and APT attacking behavior. Considering that the lateral movement of APTs heavily relies on the presence of vulnerabilities, the absence of this element may diminish the effectiveness of detection methods. To address this gap, we propose an enhanced APT detection technique that incorporates the correlation between APT attributes and network vulnerabilities. By integrating these two factors, our approach improves the detection capabilities and enhances the overall effectiveness of APT detection mechanisms.

Supplementary data

Supplementary materialis available at the *Journal of Cybersecurity* online version of the manuscript.

Acknowledgement

This work was supported by UAEU Start-Up Grant 2024 with the project code 'G00004629' and the Ministry of Higher Education Malaysia under the Transdisciplinary Research Grant Scheme (TRGS) of Grant No. "TRGS/1/2020/UNITEN/01/1/2".

Author contributions

Nur Ilzam Che Mat (Conceptualization [lead], Data curation [lead], Methodology [lead], Resources [equal], Writing – original draft [lead], Writing – review & editing [lead]), Norziana Jamil (Conceptualization [lead], Data curation [lead], Formal analysis [lead], Funding acquisition [lead], Methodology [lead], Supervision [lead]), Yunus Yusoff (Conceptualization [supporting], Data curation [supporting], Formal analysis [supporting], Methodology [supporting], Resources [supporting], Supervision [supporting], Writing – original draft [supporting], Writing – review & editing [supporting]), and Miss Laiha Mat Kiah (Conceptualization [supporting], Data curation [supporting], Formal analysis [supporting], Funding acquisition [supporting], Methodology [supporting], Resources [supporting], Supervision [supporting], Writing – original draft [supporting], Writing – review & editing [supporting])

References

1. Te Liu S, Chen YM, Lin S-J. A novel search engine to uncover potential victims for APT investigations. In: CH Hsu, X Li, X Shi, R Zheng (eds.), *Lecture Notes in Computer Science*. Vol. **8147**. Berlin: Springer, 2013, 405–16.
2. Moya JR, Decastro-García N, Fernández-Díaz R-Á. *et al.* Expert knowledge and data analysis for detecting advanced persistent threats. *Open Math* 2017;**15**:1108–22.
3. Cinar C, Alkan M, Dörterler M. A study on advanced persistent threat. In: *2018 3rd International Conference on Computer Science and Engineering (UBMK)*, 2018, 116–21. 10.1109/UBMK.2018.8566348.
4. Blumbergs B. *Technical analysis of advanced threat tactics targeting critical information infrastructure*. Cyber security Review. 2014, 1–12.
5. TrendMicro. *Securing the Pandemic-Disrupted Workplace*. 2020. [online] Available: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securing-the-pandemic-disrupted-workplace-trend-micro-2020-midyear-cybersecurity-report (16 Mac 2023, date last accessed).
6. Kushner D. The real story of Stuxnet—IEEE Spectrum. *IEEE Spectr* 2013;48–53. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (20 January 2023, date last accessed).
7. Kumar R, Kela R, Singh S. *et al.* APT attacks on industrial control systems: a tale of three incidents. *Int J Crit Infrastruct Prot* 2022;**37**:100521.
8. Daly MK. The Advanced persistent threat (or informationized force operations). *Usenix* 2009;**4**:2013–6. http://static.usenix.org/event/lisa09/tech/slides/daly.pdf.
9. Zhang Q, Li H, Hu J. A study on security framework against advanced persistent threat. *7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC)*. 2017;**Vol. 2**:128–31.
10. Husari G, Al-Shaer E, Chu B. *et al.* Learning APT chains from cyber threat intelligence. *HotSoS '19: Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*, 2019, 1–2. 10.1145/3314058.3317728.
11. Xing K, Li A, Jiang R. *et al.* A review of APT attack detection methods and defense strategies. *2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC)*. 2020, 67–70. 10.1109/dsc50466.2020.00018.
12. Grooby S, Dargahi T, Dehghantanha A. Protecting IoT and ICS platforms against advanced persistent threat actors: analysis of APT1, silent chollima and molerats. In: A Dehghantanha, KK Choo (eds.), *Hand-*

book of Big Data and IoT Security. Cham: Springer, 2019, 225–55. 10.1007/978-3-030-10543-3_10.
13. Husari G, Al-Shaer E, Ahmed M. TTPDrill: automatic and accurate extraction of threat actions from unstructured text of CTI sources. *ACM Int Conf Proc Ser* 2017;**Part F1325**:103–15.
14. Wen S, He N, Yan H. Detecting and predicting APT based on the study of cyber kill chain with hierarchical knowledge reasoning. *ACM Int Conf Proc Ser* 2017;115–9. doi: 10.1145/3171592.3171641.
15. Clio S, Han I, Jeong H. *et al.* Cyber kill chain based threat taxonomy and its application on cyber common operational picture. *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. 2018. 10.1109/CyberSA.2018.8551383.
16. Ahmed Y, Asyhari AT, Rahman MA. A cyber kill chain approach for detecting advanced persistent threats. *Comput Mater Contin* 2021;**67**:2497–513.
17. Robinson P, Lowe J. Literature reviews vs systematic reviews. *Aust NZ J Public Health* 2015;**39**:103.
18. Pahlevan Sharif S, Mura P, Wijesinghe SNR. Systematic reviews in Asia: introducing the "PRISMA" Protocol to tourism and hospitality scholars. *Quantitative Tourism Research in Asia*. 2019, 13–33. 10.1007/978-981-13-2463-5_2.
19. Hussain S, Bin Ahmad M, Uddin Ghouri SS. Advance persistent threat—a systematic review of literature and meta-analysis of threat vectors. *Adv Intell Syst Comput* 2021;**1158**:161–78.
20. Murtaza MR, Siddiqi A, Mugheri MA. *et al.* Advanced Persistent Threats Defense Techniques: A Review. *Pakistan J. Comput. Inf. Syst* 2017;**2**:53–65[Online]. Available: http://pastic.gov.pk/downloads/PJCIS/PJCIS_V2_2.pdf (3 April 2023, date last accessed)
21. Radhakrishnan K, Menon RR, Nath HV. A survey of zero-day malware attacks and its detection methodology. *TENCON 2019—2019 IEEE Region 10 Conference*. 2019;**2019-October**:533–9.
22. Navarro J, Deruyver A, Parrend P. A systematic survey on multi-step attack detection. *Comput Secur* 2018;**76**:214–49.
23. Bhat BA, Kumar R. APT: a buzzword and a reality—a bibliometric review of the literature (2010–2020). *IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys)*. 2022, 1972–9. 10.1109/HPCC-DSS-SmartCity-DependSys53884.2021.00295.
24. Luh R, Schrittwieser S, Marschalek S. TAON: an ontology-based approach to mitigating targeted attacks. *ACM Int Conf Proc Ser* 2016;303–12. 10.1145/3011141.3011157.
25. Vaismoradi T, Turunen H, Bondas T. Content analysis and thematic analysis: implications for conducting a qualitative descriptive study. *Nurs Heal Sci* 2013;**15**:398e405.
26. Braun V, Clarke V. Using thematic analysis in psychology. *Qual Res Psychol* 2006;**3**:77–101.
27. Julisch K. Mining alarm clusters to improve alarm handling efficiency. *Proc Annu Comput Secur Appl Conf ACSAC*. 2001;**2001-January**:12–21.
28. Brogi G. Real-time detection of advanced persistent threats using information flow tracking and hidden Markov models. Ph.D. Thesis, Centre d'Études et de Recherche en Informatique et Communications, Télécom Paris, 2018, http://www.theses.fr/2018CNAM1167 (21 January 2023, date last accessed).
29. Ghafir I, Hammoudeh M, Prenosil V. *et al.* Detection of advanced persistent threat using machine-learning correlation analysis. *Future Gener Comput Syst* 2018;**89**:349–59.
30. Ghafir I, Prenosil V, Hammoudeh M. *et al.* Disguised executable files in spear-phishing emails: detecting the point of entry in advanced persistent threat. *ACM Int Conf Proc Ser* 2018;2–6. doi: 10.1145/3231053.3231097.
31. Liu H, Lang B. Machine learning and deep learning methods for intrusion detection systems: a survey. *Appl Sci* 2019;**9**:4396. 10.3390/app9204396.
32. Lu J, Zhang X, Junfeng W. *et al.* APT traffic detection based on time transform. *International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*. 2017, 9–13. 10.1109/ICITBS.2016.87.
33. Pei K, Gu Z, Saltaformaggio B. *et al.* HERCULE: attack story reconstruction via community discovery on correlated log graph. *ACM Int Conf Proc Ser* 2016;**5–9-December**:583–95.
34. GhasemiGol M, Ghaemi-Bafghi A. E-correlator:an entropy-based alert correlation system. *Secur Commun Netw* 2015;**8**:822–36.
35. GhasemiGol M, Ghaemi-Bafghi A. Symantec Advanced Threat Protection. 2014, https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1039 (15 January 2023, date last accessed).
36. Friedberg I, Skopik F, Settanni G. *et al.* Combating advanced persistent threats: from network event correlation to incident detection. *Comput Secur* 2015;**48**:35–57.
37. Chia-Mei C, Guan DJ, Huang Y-Z. *et al.* Anomaly network intrusion detection using hidden Markov model. *Int J Innov Comput Inform Control* 2016;**12**:569–80.
38. Quintero-Bonilla S, del Rey AM. A new proposal on the advanced persistent threat: a survey. *Appl Sci* 2020;**10**:3874.
39. Ghafir I, Prenosil V. Malicious file hash detection and drive-by download attacks. *Adv Intell Syst Comput* 2016;**379**:661–8.
40. Hong KF, Chen CC, Chiu Y-T. *et al.* Ctracer: uncover C&C in advanced persistent threats based on scalable framework for enterprise log data. *2015 IEEE International Congress on Big Data*. 2015, 551–8. 10.1109/BigDataCongress.2015.86.
41. Adachi D, Omote K. A host-based detection method of remote access trojan in the early stage. *Lect Notes Comput Sci* 2016;**10060**:110–21.
42. Bai T, Bian H, Daya AA. *et al.* A machine learning approach for RDP-based lateral movement detection. *IEEE 44th Conference on Local Computer Networks (LCN)*. 2019;**2019-October**:242–5.
43. Joloudari JH, Haderbadi M, Mashmool A. *et al.* Early detection of the advanced persistent threat attack using performance analysis of deep learning. *IEEE Access* 2020;**8**:186125–37.
44. Mohamed N, Belaton B. SBI model for the detection of advanced persistent threat based on strange behavior of using credential dumping technique. 2021;**1**:42919–32.
45. Sexton J, Storlie C, Neil J. Attack chain detection. *Stat Anal Data Min* 2015;**8**:353–63.
46. Edr P. *ESET Enterprise*. https://www.eset.com/gh/business/endpoint-security/enterprise-inspector/ (10 February 2023, date last accessed).
47. Jain AK. Data clustering: 50 years beyond K-means. *Pattern Recognit Lett* 2010;**31**:651–66.
48. Zhang R, Huo Y, Liu J. *et al.* Constructing APT attack scenarios based on intrusion kill chain and fuzzy clustering. *Secur Commun Netw* 2017;**2017**:1–9.
49. Kawakani CT, Barbon S, Sanches Miani R. *et al.* Discovering attackers past behavior to generate online hyper-alerts. *Braz J Inf Syst* 2017;**10**:122–47.
50. Choi J, Choi C, Lynn HM. *et al.* Ontology based APT attack behavior analysis in cloud computing. *10th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*. 2015, 375–9. 10.1109/BWCCA.2015.69.
51. Han W, Xue J, Wang Y. *et al.* APTMalInsight: identify and cognize APT malware based on system call information and ontology knowledge framework. *Inf Sci (NY)* 2021;**546**:633–64.
52. Lu J, Chen K, Zhuo Z. *et al.* A temporal correlation and traffic analysis approach for APT attacks detection. *Cluster Comput* 2019;**22**:7347–58.
53. Alserhani FM. Alert correlation and aggregation techniques for reduction of security alerts and detection of multistage attack. *Int J Adv Stud Comput Sci Eng* 2016;**5**:1. http://www.ijascse.org/volume-5-issue-2/Alert_coorelation.pdf.
54. Lecci F, Cisewski J, Chazal F. *et al.* Statistical inference for topological data analysis. Ph.D. Thesis, 2014. Carnegie Mellon University, Department of Statistics, (25 January 2023, date last accessed).
55. Lv Y, Xiang S, Geng J. *et al.* An alert correlation algorithm based on the sequence pattern mining. *2015 IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*. 2016, 1146–51. 10.1109/IAEAC.2015.7428739.

56. Yan G, Li Q, Guo D. *et al.* Discovering suspicious APT behaviors by analyzing DNS activities. *Sensors (Switzerland)* 2020;**20**:1–17.
57. Lallie HS, Debattista K, Bal J. A review of attack graph and attack tree visual syntax in cyber security. *Comput Sci Rev* 2020;**35**:100219.
58. Li T, Jiang Y, Lin C. *et al.* DeepAG: attack graph construction and threats prediction with Bi-directional deep learning. *IEEE Trans Dependable Secur Comput* 2022;**20**:1–18. 10.1109/TDSC.2022.3143551.
59. Niu W, Zhang X, Yang G. *et al.* Modeling attack process of advanced persistent threat using network evolution. *IEICE Trans Inf Syst* 2017;**E100D**:2275–86.
60. Activities DNS. Discovering suspicious APT behaviors by analyzing. *Sensors* 2020;**20**:1–17.
61. Zhao G, Xu K, Xu L. *et al.* Detecting APT malware infections based on malicious DNS and traffic analysis. *IEEE Access* 2015;**3**:1132–42.
62. Karspersky. Kaspersky Anti Targeted Attack. 2022. https://content.kaspersky-labs.com/se/media/en/business-security/enterprise/Datasheet_KATA.pdf.
63. Bitdefender. 2011. https://businessresources.bitdefender.com/hubfs/Bitdefender_Ransomware_Mitigation_Technical_Solution_Brief_2021.pdf?cid=ppc|b|google|SMB-sitelink&gclid=EAIaIQobChMIyom3tqH9gQMVS1d9Ch0URAntEAAYASACEgJyI_D_BwE (20 February 2023, date last accessed).
64. Bhatt P, Yano ET, Gustavsson P. Towards a framework to detect multi-stage advanced persistent threats attacks. *IEEE 8th International Symposium on Service Oriented System Engineering*, 2014, 390–5. 10.1109/SOSE.2014.53.
65. Takey YS, Tatikayala SG, Sarma Samavedam S. *et al.* Real time early multi stage attack detection. *7th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2021, 283–90. 10.1109/ICACCS51430.2021.9441956.
66. Katipally R, Gasior W, Cui X. *et al.* Multistage attack detection system for network administrators using data mining. *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, 2010. 10.1145/1852666.1852722.
67. Al-Shaer E. *et al.* Statistical learning of APT TTP chains from MITRE ATTCK. Mlc, 2017, 103–15.