Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 19 No. 12 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijim.v19i12.47455

PAPER

The Cyber Kill Chain Methodology as a Business Defense Tool: A Systematic Review of Its Application and Efficacy

Junior E. Dávila-Huayhuapuma, Eduardo Vílchez-Roncal, Carlos A. Alvarado-Silva (✉)

Universidad Tecnológica del Perú, Lima, Perú

c21629@utp.edu.pe

ABSTRACT

This study focuses on analyzing the detection and defense of cyber-attacks on companies, emphasizing the Cyber Kill Chain (CKC) model. Examining specialized articles reveals the widespread recognition and application of this structured methodology in cybersecurity. The model proves valuable for identifying and mitigating attack stages, facilitating early detection and a more effective response to security incidents. Results indicate its notable effectiveness in scrutinizing cyber attackers' strategies throughout the attack process, with variations based on organizational size and industry. Adapting the model to specific contexts is crucial. Despite positive findings, limitations include restricted access to academic literature and potential biases in paper selection. The study recommends organizations integrate the CKC model into their cybersecurity strategies, advocating collaboration among experts, researchers, and professionals. This collaborative effort aims to address identified limitations, enhance understanding, and expand knowledge about the model's effectiveness and adaptation to diverse environments. Overcoming these challenges will strengthen the application of the CKC model in combating cyber threats, ultimately providing enhanced protection for the information and systems of companies and entities in today's digital landscape.

KEYWORDS

Cyber Kill Chain (CKC), cyberattack, cybersecurity, detection methodology, business defense

1 INTRODUCTION

Cyberattacks continue to evolve at an alarming rate, becoming increasingly sophisticated and difficult to detect. This escalation poses significant risks to organizations, governments, and individuals, particularly as digital transformation accelerates across sectors. Modern cyber threats leverage advanced tactics to exploit vulnerabilities in computer networks and systems. These vulnerabilities are often

Dávila-Huayhuapuma, J.E., Vílchez-Roncal, E., Alvarado-Silva, C.A. (2025). The Cyber Kill Chain Methodology as a Business Defense Tool: A Systematic Review of Its Application and Efficacy. *International Journal of Interactive Mobile Technologies (iJIM)*, 19(12), pp. 160–179. https://doi.org/10.3991/ijim.v19i12.47455

Article submitted 2023-12-19. Revision uploaded 2025-04-11. Final acceptance 2025-04-30.

© 2025 by the authors of this article. Published under CC-BY.

compounded by an over-reliance on perimeter-based security measures, such as predefined databases of compromise indicators, which are insufficient to counter emerging threats [1]. Despite substantial investments in cybersecurity measures, organizations continue to face an upsurge in successful attacks, underscoring the need for more robust and adaptive strategies [2].

In the year 2022, Peru experienced approximately 15 million potential cyberattacks, representing a notable 35% increase compared to the previous year. Similarly, other countries in Latin America have reported alarming statistics. For instance, Brazil recorded over 16 billion attempted cyberattacks in the first half of 2022 alone, making it one of the most targeted nations in the region. Mexico and Colombia also face significant threats, with ransomware and phishing attacks being among the most common [3]. Latin America has become a growing target for cybercriminals due to its rapid digital transformation and increased reliance on online services. According to Kaspersky, the region saw a 24% increase in ransomware attacks in 2022 compared to the previous year, while phishing attempts surged by over 30% [4]. This vulnerability is exacerbated by uneven investments in cybersecurity infrastructure across the region, where smaller organizations often lack the resources to implement advanced security measures. Governments across Latin America have started implementing policies to address these threats. For example, Mexico launched its National Cybersecurity Strategy in 2017, emphasizing the protection of critical infrastructure and the promotion of a cybersecurity culture. Brazil, on the other hand, established its National Cybersecurity Plan 2020–2023, focusing on enhancing public-private collaboration and developing local cybersecurity capabilities. Despite these efforts, the region remains highly vulnerable, with many organizations failing to adopt proactive measures against sophisticated threats [5].

Recent years have also seen a dramatic increase in cyberattacks targeting critical infrastructure, enterprises, and individual users. For instance, crimeware-as-a-service (CaaS) has enabled malicious actors to scale their operations by providing tools for ransomware, phishing, and other attacks. These services have significantly contributed to the exponential growth of cybercrime globally, particularly in regions such as Latin America, where cyberattacks surged by 600% during the COVID-19 pandemic [1]. This surge has been attributed to insufficient investments in modern information technology infrastructure and cybersecurity measures, leaving many organizations vulnerable to increasingly sophisticated threats.

Moreover, new methodologies integrating cloud computing and advanced machine learning models have shown promise in enhancing the detection and mitigation of these threats. A study combining the Cyber Kill Chain (CKC) framework with cloud-based machine learning (CML) demonstrated significant improvements in identifying and preventing website phishing attacks, achieving detection rates of over 97% [3]. Such approaches highlight the potential of integrating theoretical models with cutting-edge technologies to enhance cybersecurity capabilities.

The increasing interconnectivity of devices in environments such as smart cities and Industry 4.0 has further expanded the attack surface for cyber threats. Smart cities, for instance, rely heavily on information and communication technologies (ICTs) to optimize urban management and enhance residents' quality of life. However, these technologies also introduce new vulnerabilities, making robust cybersecurity measures indispensable [6]. Studies have identified critical

dimensions of security risks in smart cities and proposed mitigation strategies to address these challenges [7]. Similarly, the adoption of advanced manufacturing technologies in Industry 4.0 has introduced unique cybersecurity challenges, particularly in safeguarding critical assets against attacks targeting confidentiality, integrity, and availability [2].

Understanding the behavior of cyber threats and their life cycle is critical for developing effective defenses. The CKC methodology offers a structured framework to analyze the stages of a cyberattack, from reconnaissance to execution, and enables organizations to implement adaptive controls and countermeasures. By studying the stages, techniques, and methods employed by attackers, cybersecurity professionals can better anticipate and neutralize threats [6]. Additionally, integrating insights from related works, such as the mapping of Open-Source Intelligence (OSINT) tools to the CKC framework, provides practical guidance on how these tools can be leveraged to improve situational awareness and defense strategies [8].

This study aims to build upon this foundation by analyzing the CKC methodology's utility in cyberattack detection and defense. It will include an examination of its application across diverse contexts, from protecting critical infrastructure to mitigating threats in smart cities and advanced manufacturing environments. The study also seeks to address gaps in existing literature by exploring how these strategies can be tailored to specific organizational and sectoral needs, thereby enhancing their practical relevance and effectiveness. Through this comprehensive analysis, the research aspires to provide actionable insights and recommendations for organizations seeking to bolster their cybersecurity postures against an ever-evolving threat landscape.

2 METHODOLOGY

2.1 Search strategy

The methodology employed in this study is founded on a systematic qualitative analysis, facilitating the presentation of information and evidence in a descriptive fashion, without the requirement for statistical analyses, which are not addressed in this section of the study. Additionally, the population, intervention, comparison, outcome (PICO) methodology was utilized to formulate specific questions, aiding in acquiring a precise comprehension of the gathered information and in precisely defining the research study's topic.

The choice of the PICO methodology in this study stems from its ability to structure research questions clearly and specifically, facilitating the identification of key components in studies related to the CKC. PICO, widely utilized in systematic reviews, breaks down the problem into concrete elements such as PICO, providing a rigorous and replicable methodological approach. In the context of this study, using PICO ensures that the questions align with the specific objectives of the study, helping to narrow the search for relevant literature and objectively evaluate the benefits of the CKC model compared to other cybersecurity methodologies. This structure not only enhances precision in retrieving information but also ensures that the extracted data is directly applicable to the organizational and cybersecurity environments targeted by the study.

Regarding the process of retrieving publications, advanced tools were employed to perform searches in reputable databases such as Scopus. During this process, Boolean operators and keywords, pre-selected under the PICO framework, were applied to ensure the relevance of the results. Once publications were identified, a preliminary analysis of titles and abstracts was conducted to determine their pertinence. Duplicated documents were removed using automated detection tools, followed by manual review to confirm the exclusion of repeated works. During the screening phase, exclusion decisions were based on clearly defined criteria, such as the absence of references to the CKC model or a lack of empirical evidence. This approach combined technical rigor and methodological precision, ensuring that only high-quality, relevant studies were included in the final analysis, thereby reinforcing the validity and reliability of the findings presented.

The results of the employed PICO strategy are provided below:

1. PICO Question: How can the CKC methodology assist in detecting and defending against attacks targeting companies and entities?
2. PICO components: Once the PICO question is identified, sub-questions are generated to break down the overarching query. This process enables the extraction of more specific components, providing precise details for a thorough and accurate search. In this study, the PICO components have been utilized without taking into account additional factors such as context and time interval.

Below are the questions posed:

a) Population: Identify the specific population or target group involved in the application of the model. Are there variations in the effectiveness of the CKC model based on the size or industry of the companies and entities?
b) Intervention: Describe the actions or measures taken when implementing the model. How is the CKC model utilized to detect and analyze cyberattacks?
c) Comparison: Contrast the CKC model with other cybersecurity approaches or methodologies. Are there studies or success stories illustrating the effectiveness of the CKC model compared to other cybersecurity approaches?

Table 1. Keywords according to PICO method

PICO Elements	Keywords	Search Terms
P (Patient/Population)	Companies and entities	Companies, Entities, Organizations, Technological infrastructures
I (Intervention)	Cyber Kill Chain model for attack detection and defense	Cyber Kill Chain, Detection and defense strategies, Security methodologies, Mitigation processes
C (Comparison/Control)	Comparison with other attack detection and defense methods	Alternative methodologies, Detection and defense models, Traditional security approaches, Existing protection solutions
O (Outcomes)	Benefit of the Cyber Kill Chain model for attack detection and defense	Risk reduction, Attack prevention, Early detection, Threat mitigation

d) Result: Examine the results or impacts obtained when applying the model. What benefits have been observed in using the CKC model in terms of early detection of attacks and reduction of their impact?

3. Selected keywords: In line with the PICO methodology, specific keywords have been chosen to conduct a precise and comprehensive systematic investigation. These keywords are crucial for obtaining results that are relevant and pertinent to the research at hand (refer to Table 1).

2.2 PRISMA Methodology

To conduct an effective search, an equation has been formulated by combining the selected keywords through the use of Boolean operators. This equation has been designed to establish a proper connection between search terms, as illustrated below: (TITLE-ABS-KEY("Cyber Kill Chain" OR "Detection and defense strategies" OR "Security methodologies" OR "Mitigation processes") AND TITLE-ABS-KEY("Risk reduction" OR "Attack prevention" OR "Early detection" OR "Threat mitigation") OR TITLE-ABS-KEY("companies" OR "entities" OR "organizations" OR "Technological infrastructures")).

Table 2. Inclusion and exclusion criteria

Inclusion	Exclusion
Scientific and technical articles addressing the detection and defense of cyber-attacks on companies and entities.	Articles not centered on the detection and defense of cyber-attacks on companies and entities.
Articles specifically discussing the application of the Cyber Kill Chain Model in detecting and defending against attacks.	Studies not mentioning or unrelated to the Cyber Kill Chain Model.
Studies presenting empirical research, experiments, case studies, or data analysis related to the utilization of the Cyber Kill Chain Model in companies and entities.	Unreliable or non-peer-reviewed sources, such as non-specialist blogs or non-scientific content.
Articles offering quantitative and qualitative evidence or results regarding the effectiveness of the Cyber Kill Chain Model in detecting and defending against attacks.	Posts that are outdated or based on obsolete versions of the Cyber Kill Chain Model.
	Studies or publications in languages other than English or Chinese.
Research covering various aspects of the Cyber Kill Chain Model, including its stages, tools, or related techniques.	Studies or publications dated earlier than 2018.
	Studies and publications unrelated to Computer Engineering.

1. Inclusion and exclusion criteria: Following the execution of the search formula on the selected database, a thorough analysis was conducted to identify the primary inclusions and exclusions in the results. This process enabled us to comprehend which terms and criteria were yielding the most relevant documents and which ones were producing unwanted or irrelevant results (refer to Table 2).
2. Study selection process: In the initial exploration of the Scopus database, 173 documents were gathered and subjected to an initial review. Subsequently, the PRISMA selection process was applied (see Figure 1), utilizing inclusion and exclusion criteria. This process yielded 69 documents deemed suitable for the research.

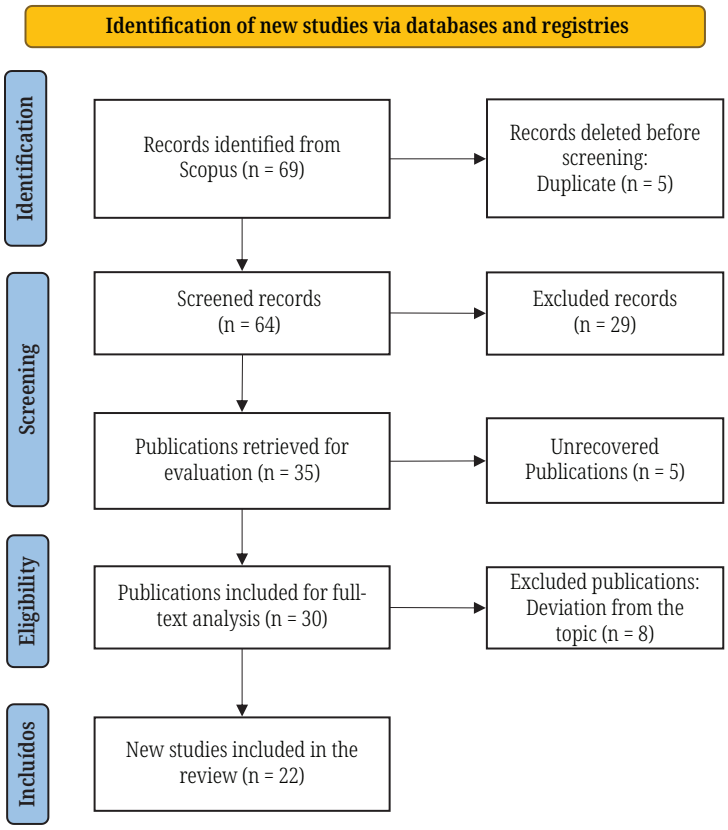

Fig. 1. Identification diagram of new studies

The titles and abstracts of these documents underwent screening to determine preliminary relevance and to eliminate those not meeting the inclusion criteria. Five duplicate documents were identified and removed. A more detailed review, involving a deeper examination of inclusion and exclusion criteria, resulted in the exclusion of an additional 29 papers.

After completing the publication recovery activities, five unrecovered publications were identified, and eight of the recovered ones contained information unrelated to the central topic of the investigation. Following this selection process, a total of 22 documents relevant to the research were obtained.

3 RESULTS

The results obtained through the chosen methodology, search equation, and the application of inclusion and exclusion criteria have furnished pertinent information for the advancement of this study. This process has allowed for the identification of a meticulous selection of documents that align with the established inclusion and exclusion criteria, ensuring the relevance and reliability of the information to be utilized in addressing the project objectives.

3.1 Descriptive analysis of the selected articles

In the analysis of the selected articles, it has been observed that, starting in 2015, there was a growing interest in research related to the CKC. Specifically, in 2018, 11 publications were carried out, while, in the following year, 2019, this figure

increased to 15 publications. However, in 2020, a decrease was recorded with only 10 publications, and in 2021, it recovered slightly with 13 publications. In 2022, the number of publications decreased by 1, and as of the current date of this year, 8 additional publications have been made.

In the subsequent figure (see Figure 2), the number of articles published annually is illustrated by a graph, reflecting the evolution of research related to the PRISMA methodology process.

These findings can provide valuable insight into the trend and academic interest surrounding the topic of the CKC over the years, helping to contextualize the importance and relevance of this study in the field of study.

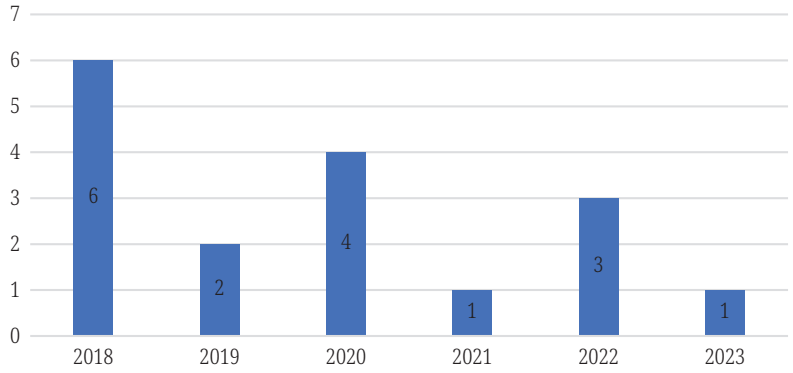

Fig. 2. Annual publication rate of academic research on Cyber Kill Chain

3.2 Types of companies or organizations that suffer cyber attacks

In the current digital age, technology plays a fundamental role in our daily activities, but it also presents significant challenges for companies and organizations due to the increasing threat of cyberattacks [7]. Cybercriminals exploit security vulnerabilities to access sensitive information, disrupt critical operations, and inflict substantial financial damage, as noted by [8]. Not all companies or organizations are equally susceptible to these attacks, so it is vital to comprehend the primary objectives of cyber-attacks. Table 3 present an overview of these objectives based on the selected and reviewed articles.

Table 3. Impact of cyberattacks by organization type and context

Type of Company or Organization	Article Title	Author	How Does it Impact?
Not mentioned	Fronesis: Digital Forensics-Based Early Detection of Ongoing Cyber-Attacks	[1]	Leading to the exposure of sensitive data and a cascade of vulnerabilities affecting multiple systems
Government Organizations	Reducing False Negatives in Ransomware Detection: A Critical Evaluation of Machine Learning Algorithms	[2]	Multimillion-dollar financial losses and significant disruptions to business operations
Companies in general	Data Centre Risk Analysis Using ISO 31000:2009 Framework	[3]	Lead to risks such as service interruptions, loss of critical data, and business continuity issues in technology-driven organizations
Companies in general	Secure mitigation and migration of virtual machines over hybrid cloud hypervisors infrastructure	[4]	Compromise sensitive data and critical services, undermining trust in cloud infrastructure environments

(Continued)

Table 3. Impact of cyberattacks by organization type and context *(Continued)*

Type of Company or Organization	Article Title	Author	How Does it Impact?
Railway Companies	Predictive model for multistage cyber-attack simulation	[5]	Disruptions in operational efficiency, passenger services, and infrastructure reliability.
Organizations	Risk based approach in scope of cybersecurity threats and requirements	[6]	Data breaches, system outages, and operational slowdowns.
Small companies	A framework for producing effective and efficient secure code through malware analysis	[7]	Encrypting critical data and demanding ransoms, permanent data loss, customer trust erosion, and significant financial strain.
Railway Companies	Railway defender kill chain to predict and detect cyber-attacks	[8]	Unauthorized control of systems like ticketing and signaling, compromising passenger safety and business continuity
multimedia service company	Modified cyber kill chain model for multimedia service environments	[9]	Leading to the exfiltration of sensitive data and financial losses, system failures and unauthorized access.
Not mentioned	A Risk Mitigation Framework for Information Technology Projects: A Cultural Contingency Perspective	[10]	Cyberattacks can derail project timelines, inflate costs, and compromise data integrity
Organizations	Modeling attack activity for integrated analysis of threat information	[11]	Compromising several points within their networks, making early detection more difficult and increasing exposure to advanced threats
Banking Companies	A cyber kill chain-based taxonomy of banking Trojans for evolutionary computational intelligence	[12]	Leading to stolen credentials, financial theft, and reputational damage
Not mentioned	An integrated cyber security risk management approach for a cyber-physical system	[13]	Lead to service disruptions, operational inefficiencies, and regulatory violations
Government Organizations	Automated detection of the early stages of cyber kill chain	[14]	Significant data, financial, and reputational losses
Organizations	Defining network exposure metrics in security risk scoring models	[15]	Data breaches, denial-of-service attacks, and prolonged system downtime, compromise the confidentiality, integrity, and availability of critical systems
Companies with critical infrastructure	Secure cyber deception architecture and decoy injection to mitigate the insider threat	[16]	Exploit legitimate access to cause damage, including data theft, sabotage, and operational disruption
military aviation	Architecture for the cyber security situational awareness system	[17]	Leads to delays in identifying and mitigating threats, increasing the risk of widespread disruption and data loss
Companies in general	Technical aspects of cyber kill chain	[18]	Financial losses and reputational damage are common consequences
Companies in general	Web engineering security (WES) methodology	[19]	Loss of confidential data and operational disruptions
Companies in general	Incorporating a knowledge perspective into security risk assessments	[20]	Unauthorized access and exploitation of critical business processes.
Organizations	Impact and key challenges of insider threats on organizations and critical businesses	[21]	Compromise the security principles of confidentiality, integrity, and availability, especially in critical infrastructure sectors
Not mentioned	Modelling Hybrid Cyber Kill Chain Wen	[22]	Loss of integrity in critical systems and unauthorized access to valuable data

In this study, an exhaustive examination of multiple review articles has been conducted to identify the types of companies and organizations targeted by cyber-attacks (refer to Table 3). These attacks are noted for their increasing level of specificity, sophistication, and persistence, as outlined in the study by [9]. Based on this data, a tally has been conducted, and the corresponding percentages have been calculated to ascertain which types of companies are most frequently impacted by these attacks.

The findings unveiled the distribution of cyberattacks aimed at each type of company or organization. These percentages are crucial for comprehending which sectors encounter the most significant cybersecurity challenges, enabling us to make more informed decisions to bolster protective measures.

The accompanying Figure 3 illustrates the proportions of attacks categorized by the type of company or organization, considering information extracted from 20 selected articles. These findings are crucial for obtaining a comprehensive overview of trends and challenges in the cybersecurity domain faced by various sectors, and they contribute significantly to research in the field of protection against cyberattacks.

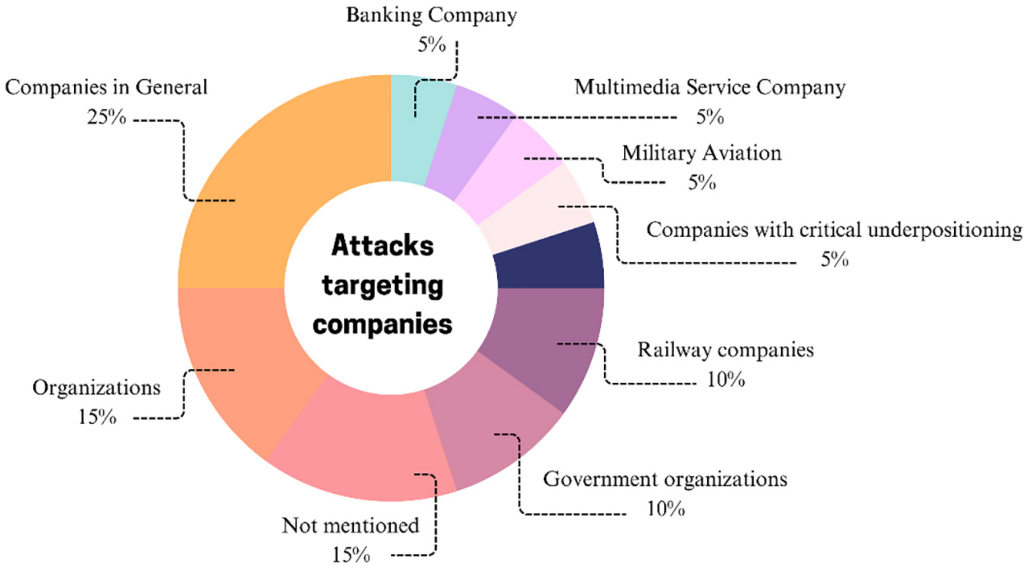

Fig. 3. Distribution diagram of attacks directed at companies and organizations according to industry (%)

3.3 Methodologies used for the detection and analysis of cybersecurity attacks

Securing information and systems from potential online threats necessitates the effective detection and analysis of cybersecurity attacks. In a continually evolving digital environment, having appropriate methodologies to identify and understand these attacks in a timely manner is of vital importance [24]. In the development of this study, a comprehensive analysis of the most commonly used methodologies for the detection and analysis of cybersecurity attacks has been conducted. To present the results in a clear and visually relevant manner, a bar graph representation has been created, illustrating the frequency of use of each methodology.

Figure 4 offers a snapshot of the preferred and widely adopted methodologies by cybersecurity professionals. Examining these trends provides greater insight into the most effective tools and approaches to combat and mitigate cyberattacks. Similarly, the bar graph summarizes the most commonly used methodologies for the detection and analysis of cybersecurity attacks, based on the articles reviewed in this study.

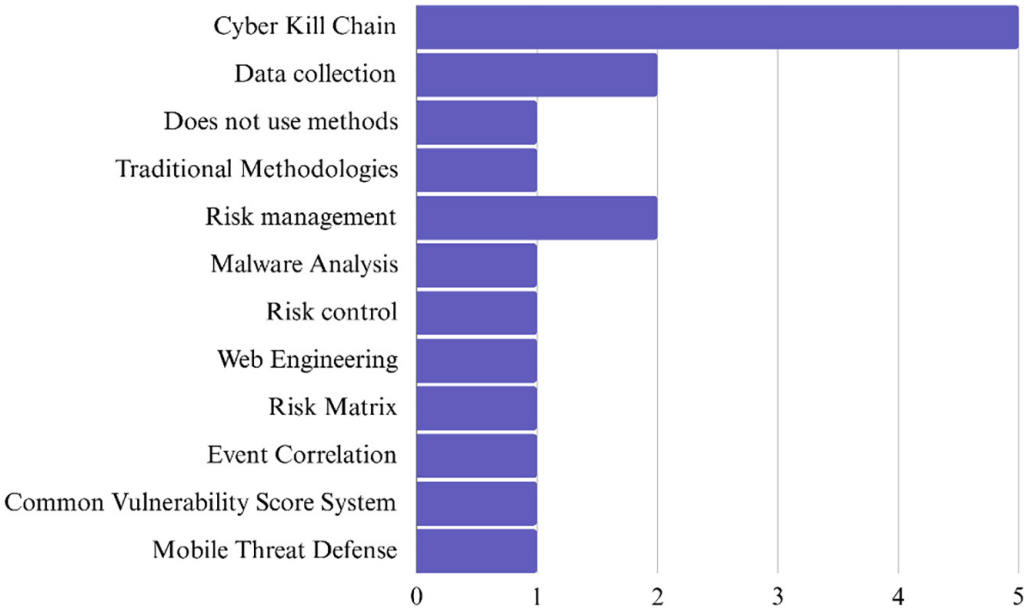

Fig. 4. Most used cybersecurity detection and analysis methodologies

These results are crucial for contributing to the advancement of knowledge in the field of cybersecurity and providing a clear overview of current practices in the fight against cyber threats. After detailing the methodologies used for the detection and analysis of cybersecurity attacks, it is emphasized that the most widely used and recognized methodology by professionals in the field is the so-called "Cyber Kill Chain."

This methodology offers a structured and systematic approach to understanding the sequence of a cyberattack, enabling the identification and effective neutralization of the stages in the attack cycle.

The popularity of the CKC methodology stems from its ability to provide a holistic view of attacks, empowering cybersecurity specialists to take proactive measures to strengthen defenses and protect information systems. The prominence of this methodology in the cybersecurity community underscores its relevance in the battle against online threats and its contribution to a more robust and efficient approach to protecting against cyberattacks.

3.4 Types of cybersecurity attacks used

In the field of cybersecurity, various methodologies are employed to detect and analyze cyberattacks. Each of these methodologies has been developed and adapted to counter different types of attacks [19]. In this section, the relationship between each methodology and a specific type of attack will be explored, with the goal of understanding how they are applied in practical contexts.

Due to the continued evolution and complexity of cyberattacks, detection and analysis methodologies have also had to adapt to meet new challenges. Each type of attack possesses its own characteristics, techniques, and objectives, necessitating specific approaches for effective detection and analysis [22].

In the conducted analysis, it has been identified that each methodology is particularly associated with a specific type of attack. These relationships highlight how each methodological approach is designed to address the key aspects of a given type of attack and provide an appropriate response. Table 4 presents the selected methodologies and their relationship with a specific type of attack.

Table 4. Keywords according to PICO method

Methodology	Type of Attack
Traditional methodologies	Phishing
Data collection	Ransomware
They do not use methods	Unidentified
They do not use methods	Unidentified
Cyber Kill Chain Methodology	cyber attacks
Risk management process	cyber attacks
Malware analysis	Generic malware
Cyber Kill Chain Methodology	Phishing
Cyber Kill Chain Methodology	Advanced Persistent Threat (APT)
Risk control	Unidentified
Cyber Kill Chain Methodology	Targeted and sophisticated attacks
Cyber Kill Chain Methodology	Advanced Persistent Threat (APT)
Risk matrix	Unidentified
Event Correlation	cyber attacks
Punctuation system	cyber attacks
Applying Moving Target Defense (MTD)	Network Mutations
Data collection	cyber attacks
Cyber Kill Chain Methodology	Targeted and sophisticated attacks
Web Engineering Security	WEB attacks
Security risks	Generic malware

Understanding the relationship between each methodology and a type of attack is a crucial factor for cybersecurity professionals. It enables them to adopt more focused and effective approaches in the detection and analysis of specific threats [25]. By comprehending the characteristics and techniques associated with each type of attack, organizations can enhance their ability to prevent and respond more effectively to cyberattacks in today's digital environment.

In this context, the figure presented below (see Figure 5) summarizes the most frequently used attacks based on the review of selected articles. This visual representation provides an overview of the most relevant types of attacks, allowing cybersecurity professionals to concentrate their efforts on addressing these specific challenges and improving the protection of information and systems within their organizations.

This figure serves as a valuable visual tool, highlighting the most significant cyberattacks and offering a solid foundation for understanding the tactics employed by malicious actors. Through a meticulous analysis of this information, cybersecurity professionals and organizations can fortify their defense and response strategies, concentrating on the highest-risk areas and implementing specific measures to mitigate these threats. By discerning the key patterns and characteristics of the attacks presented in the figure, experts can identify weaknesses in their systems and apply customized solutions to protect their infrastructure and data more efficiently. The information encapsulated in this figure will enable organizations to make informed decisions about resource allocation and the implementation of more effective cybersecurity measures.

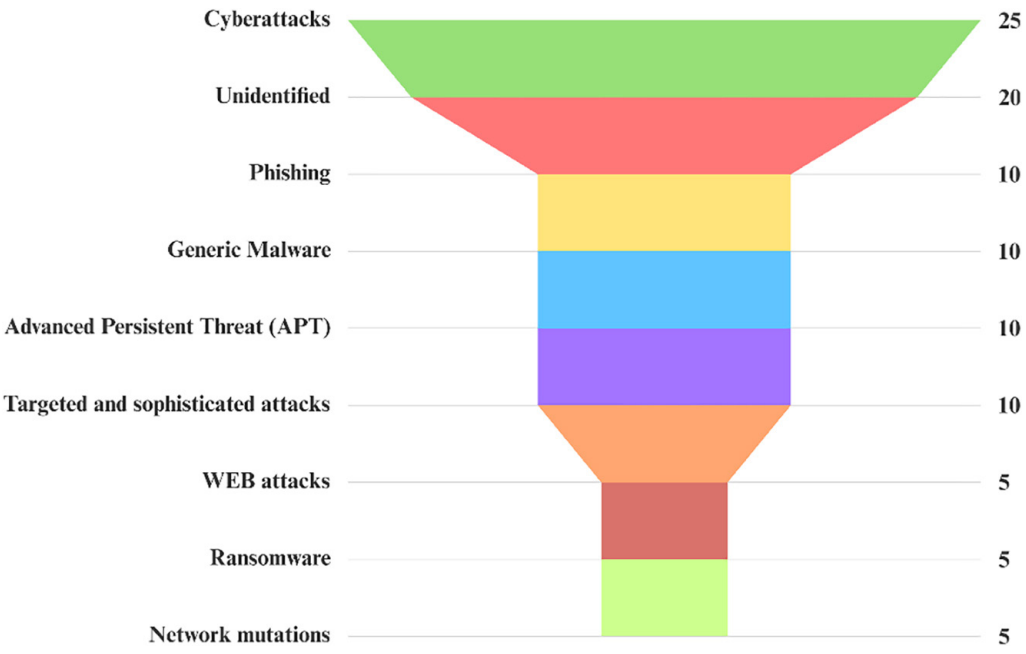

Fig. 5. Diagram representing the most used attacks (%)

3.5 Main findings

The CKC model has proven to be highly effective in identifying, mitigating, and preventing cyber threats through its structured, stage-based approach (see Figure 6). By breaking down the lifecycle of an attack into actionable steps—reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objectives—it provides organizations with a clear roadmap for defense. Its application in environments such as smart manufacturing is particularly beneficial, as it helps reduce vulnerabilities in critical systems and enhances the resilience of industrial operations [26]. This effectiveness is amplified when combined with complementary strategies such as network segmentation and automated response systems.

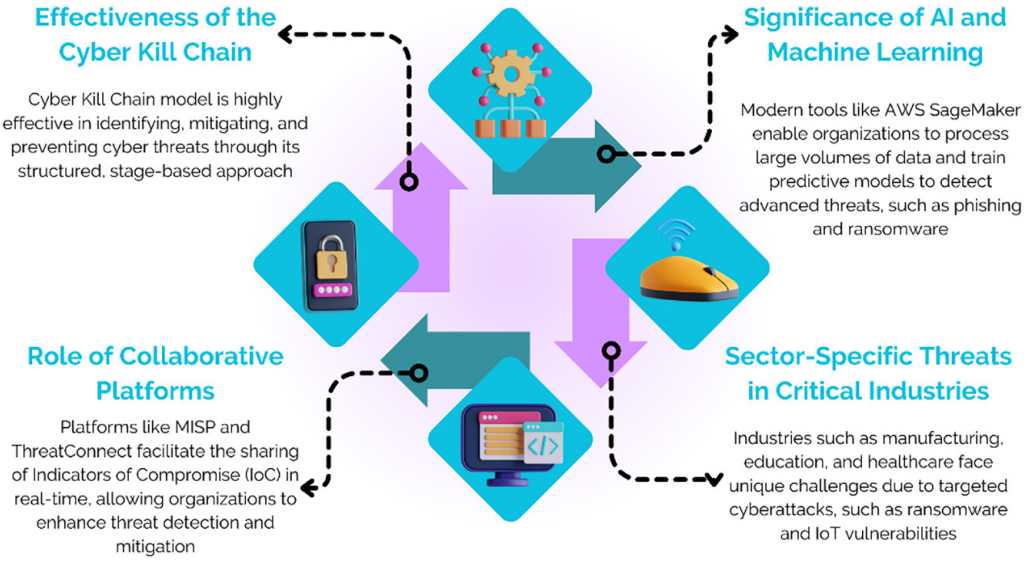

Fig. 6. Key insights on cyber threat mitigation and industry-specific risks

Network segmentation architectures, when paired with automated containment mechanisms, are instrumental in reducing the attack surface and isolating sensitive assets. These systems are particularly effective in industrial and wireless environments, where the continuity of operations is critical. By automating threat response actions, organizations can minimize the impact of potential breaches, thus reinforcing their overall cybersecurity posture [27]. To further enhance these efforts, the use of artificial intelligence and machine learning provides unprecedented capabilities for real-time detection and prediction of cyberattacks.

Modern technologies, such as AWS SageMaker, enable organizations to process large volumes of data and train predictive models to identify sophisticated threats such as phishing and ransomware. These tools allow for the detection of complex patterns and anomalies, greatly improving the speed and accuracy of threat identification. When integrated with collaborative platforms, the effectiveness of these technologies can be further enhanced [3].

Collaborative threat intelligence platforms, such as MISP and ThreatConnect, facilitate the sharing of indicators of compromise (IoC) across organizations, enabling real-time threat detection and mitigation. The ability to pool knowledge and resources through these platforms empowers organizations to stay ahead of emerging threats and adapt their defenses proactively [28]. This collaboration is particularly crucial in industries such as manufacturing, education, and healthcare, where specific threats target critical infrastructure.

In industries such as these, tailored cybersecurity strategies are essential. Common threats, including ransomware, phishing, and IoT vulnerabilities, exploit the interconnected nature of industrial systems, making sector-specific defenses a priority [5]. Addressing these challenges also requires a comparison of traditional detection methodologies and modern approaches to highlight their respective strengths and limitations.

While traditional methods rely on predefined rules, modern techniques, such as deep learning algorithms, adapt dynamically to evolving threats. These advanced systems are superior in detecting complex attack patterns and responding to emerging cyber challenges in real time [29]. However, the adoption of such technologies also brings with it challenges related to data management and analysis.

The integration and processing of large-scale data remain significant obstacles for many organizations. To address this, advanced analytics tools and cloud platforms are increasingly being used to structure and analyze data efficiently, enabling faster and more accurate threat detection [17]. Nevertheless, the success of these technologies depends on the human element—education and training within organizations.

A strong cybersecurity culture is built on continuous awareness and training programs. Employees must be equipped to recognize tactics such as phishing and social engineering, which are often the weakest points in an organization's defenses. Regular training ensures that employees are not only aware of the risks but also prepared to act as the first line of defense against potential threats [8]. Such proactive measures are supported by studies demonstrating the economic benefits of robust cybersecurity investments.

Investing in cybersecurity technologies can prevent significant financial losses and improve organizational resilience. By minimizing downtime and protecting critical assets, organizations can safeguard their operations and maintain trust with stakeholders [11]. This is particularly important in the face of rapidly evolving cyber threats.

The advancement of cyberattacks, driven by attackers leveraging emerging technologies, requires organizations to continuously update their defenses. Moreover, international collaboration is essential to create comprehensive strategies for combating these threats and ensuring a secure global cybersecurity ecosystem [30].

4 DISCUSSION

4.1 Answers to research questions

1. How can the CKC model assist in detecting and defending against attacks that occur in companies and entities? The CKC model offers a structured and systematic approach to understanding the sequence of a cyber-attack. By proactively identifying and neutralizing the stages of the attack cycle, this model helps prevent and mitigate potential damage to the critical infrastructure and data of companies and entities [31]. Additionally, it enables the early detection of attacks, facilitating a faster and more effective response to security incidents.
2. Are there variations in the effectiveness of the CKC model based on the size or industry of the companies and entities? Yes, there are differences in the effectiveness of the CKC model depending on the size and industry of the companies and entities. Organizations with greater resources and capabilities in cybersecurity can apply this model more efficiently [32]. Additionally, certain industries may be more susceptible to specific types of attacks, influencing the adaptation and success of the model in different contexts.
3. How is the CKC model utilized to identify and analyze attacker tactics and techniques? The CKC model is employed to break down the attack process into stages, enabling the identification of specific patterns and characteristics associated with each type of attack. Through the analysis of tactics and techniques employed by attackers at each stage, a more profound understanding of the methods used by malicious actors is attained [33]. This, in turn, facilitates a more effective and strategic response to defend against future attacks.
4. Are there any studies or success stories that demonstrate the effectiveness of the CKC model compared to other cybersecurity approaches? Yes, there are studies and success stories that showcase the effectiveness of the CKC model compared to other cybersecurity approaches. These studies have emphasized how the implementation of this methodology has resulted in enhanced early detection of attacks, improved incident response, and a reduction in the impact of attacks on organizations [34].
5. What benefits have been observed when using the CKC model in terms of early detection of attacks and the reduction of their impact? The benefits observed when using the CKC model include early detection of attacks, enabling a faster and more effective response to security incidents. By understanding the techniques employed by attackers at each stage of the attack cycle, organizations can fortify their defenses and minimize the impact of attacks on their critical infrastructure and data [35].

4.2 Practical implications

The results of this study have direct practical applications across various settings. In education, the proposed inclusive strategies can be employed to develop programs specifically designed for neurodiverse students, optimizing learning through multisensory and adaptive methods. This approach reduces educational barriers by promoting a more accessible and equitable learning environment. For instance, implementing multisensory resources could inspire early intervention programs that incorporate tactile, visual, and auditory activities to strengthen cognitive and social skills in students [16].

In the technological sector, the findings provide valuable guidance for enhancing cybersecurity in critical systems. For example, employing risk lifecycle strategies, such as business impact analysis in smart manufacturing systems, can mitigate vulnerabilities in complex industrial environments. This approach is critical for protecting sensitive data and improving operational resilience against cyberattacks. Research in Industry 4.0 environments highlights the importance of safeguarding data confidentiality, integrity, and availability to avoid critical disruptions in supply chains [8–14].

Additionally, in organizational contexts, the findings emphasize the importance of integrating collaborative tools such as threat intelligence-sharing platforms to enhance risk detection and mitigation. Platforms such as MISP and ThreatConnect have proven effective in enabling organizations to share IoC and strengthen their cybersecurity defenses. These strategies can help prevent attacks through real-time monitoring and early anomaly detection, as demonstrated in recent studies on the use of collaborative platforms for threat management [14–17].

From a policy perspective, the findings underscore the need to design more robust regulatory frameworks that promote the adoption of inclusive and secure practices in educational and technological environments. For instance, creating standards to ensure equitable access to adaptive technologies and inclusive digital tools could significantly transform the educational and professional landscapes for vulnerable populations [11].

In business, organizational policies can prioritize cybersecurity training and the use of artificial intelligence tools to optimize processes. For instance, machine learning models deployed via cloud computing platforms such as AWS SageMaker have demonstrated superior efficiency in phishing attack detection, achieving accuracies exceeding 95% with minimal processing times [36].

Finally, in a social context, inclusive educational programs leveraging 3D printing technologies to create personalized teaching materials can provide innovative solutions for students with disabilities. This approach, as evidenced in studies on neurodiversity and multisensory learning, not only enhances educational equity but also fosters more interactive and meaningful learning experiences.

4.3 Organizational limitations in cybersecurity

One of the most significant limitations faced by organizations in cybersecurity is the lack of financial resources. This is particularly evident in small and medium-sized enterprises (SMEs), which often operate on limited budgets that prevent them from investing in advanced cybersecurity tools, such as those based on artificial intelligence and machine learning. As a result, these organizations remain vulnerable to sophisticated cyber threats.

Another critical challenge is the shortage of skilled cybersecurity professionals. Many organizations lack personnel with the expertise necessary to implement advanced models such as the CKC or to effectively use collaborative threat intelligence platforms. This skills gap reduces the overall effectiveness of cybersecurity strategies and limits organizations' ability to respond to emerging threats [2].

The reliance on outdated technologies also poses a significant risk. Many businesses still use legacy systems that were not designed to handle modern cyber threats. These systems lack advanced security features and often become easy targets for attackers, further exacerbating organizational vulnerabilities [22].

A pervasive issue across industries is the lack of a strong cybersecurity culture. Employees often remain unaware of the risks associated with cyber threats such as phishing or ransomware, making them the weakest link in an organization's

defense. Without regular training and awareness programs, employees are more likely to fall victim to these attacks, compromising the organization's security.

Organizations also struggle with the integration of cybersecurity solutions. Managing multiple tools without a unified strategy often leads to inconsistencies in threat detection and response. This fragmentation undermines the effectiveness of cybersecurity efforts and creates potential blind spots for attackers to exploit.

In certain industries, such as manufacturing, education, and healthcare, organizations often underestimate risks specific to their sectors. Critical infrastructure in these fields is frequently targeted by cyberattacks, and failure to address these unique threats increases their vulnerability [3].

Additionally, there is a lack of inter-organizational collaboration. Many companies fail to leverage platforms such as MISP or ThreatConnect for sharing threat intelligence. This missed opportunity prevents organizations from learning from incidents experienced by others and limits the development of collective defenses.

The analysis of large volumes of data in real-time is another pressing challenge. Organizations often lack the tools and methodologies to process and analyze data efficiently, which hampers their ability to detect and respond to cyberattacks quickly [16].

Resistance to change is another barrier to enhancing cybersecurity. The adoption of new technologies and practices is frequently slowed by organizational inertia, stemming from a lack of understanding or concerns about upfront costs. This reluctance to evolve leaves organizations ill-prepared for modern cyber threats.

Finally, legal and regulatory complexities pose significant challenges for organizations operating across multiple jurisdictions. Compliance with diverse laws and regulations surrounding data management and cybersecurity often complicates the implementation of effective strategies, creating additional hurdles for global organizations [33].

Addressing these limitations requires a multifaceted approach that includes increased investment, enhanced training, better collaboration, and the adoption of modern technologies and practices tailored to the unique needs of each organization.

4.4 Recommendations

To effectively implement the CKC model, businesses should adopt a strategic and structured approach tailored to their specific operational needs. The following recommendations provide a comprehensive guide for organizations seeking to enhance their cybersecurity posture using this model.

Firstly, it is essential to strengthen the reconnaissance phase by deploying advanced artificial intelligence and machine learning tools to monitor anomalous patterns in network behavior. These technologies can proactively identify potential malicious actors before threats materialize. For example, cloud platforms such as AWS SageMaker can be used to process large-scale data in real-time and train predictive models capable of detecting early signs of cyber threats [30].

Secondly, businesses should optimize their preparation and delivery defenses by conducting regular ethical hacking exercises. These simulations can help uncover vulnerabilities within their systems and ensure timely patching of security flaws. Leveraging tools such as Nessus and Nmap for vulnerability scanning can provide actionable insights into system weaknesses, enabling proactive remediation efforts [71].

Thirdly, real-time detection capabilities must be prioritized to minimize the impact of cyber incidents. Organizations should consider adopting collaborative platforms

such as MISP and ThreatConnect to share and receive IoC in real-time. This collective approach fosters proactive threat management by allowing companies to stay ahead of emerging cyber threats [6].

Furthermore, it is crucial to bolster containment and mitigation strategies. Businesses should implement network segmentation to isolate compromised areas and limit the spread of threats. Additionally, automating response mechanisms can help organizations swiftly neutralize attacks. For instance, incorporating software-defined networking (SDN) architectures alongside OODA Loop methodologies has proven effective in addressing threats in wireless environments [10].

Cultivating a cybersecurity culture within the organization is equally important. Regular training sessions should be conducted to educate employees on safe practices, such as recognizing phishing emails and avoiding common social engineering traps. Simulating real-world attacks within the CKC framework can raise awareness and improve the organization's overall security posture [24].

Lastly, businesses should establish clear metrics to continuously monitor and evaluate the effectiveness of the CKC model. Key performance indicators (KPIs) such as the number of mitigated incidents, response times, and associated costs can provide valuable feedback for refining strategies. Tools such as AWS CloudWatch can automate the generation of reports on network status and detected threats, offering insights for ongoing improvements [28].

4.5 Possible study perspectives

Future research could delve into analyzing the specific motivations and objectives behind cyberattacks targeting diverse industries and organizational types. By exploring these motivations, researchers could gain a deeper understanding of the underlying factors that render certain sectors, such as healthcare, finance, or manufacturing, more vulnerable to cyber threats. This analysis would not only help identify high-risk areas but also inform the development of tailored mitigation strategies for each sector.

Another promising avenue for investigation involves exploring emerging and evolving methodologies for the detection, prevention, and analysis of cyber-attacks. Research in this area could focus on how novel approaches, such as artificial intelligence, machine learning, and real-time threat intelligence platforms, address both current and anticipated cybersecurity challenges. This would offer invaluable insights into advancing threat defense mechanisms and enhancing response practices across a broad spectrum of scenarios.

Furthermore, conducting comparative studies of different methodologies across various industries and contexts could provide critical data on their relative effectiveness. For example, such research could compare traditional rule-based systems with AI-driven solutions or assess how the CKC model performs in specific industries such as critical infrastructure, retail, or education. These comparative analyses would help cybersecurity professionals make more informed decisions about selecting the most suitable approaches based on their unique operational environments and risk profiles.

Finally, expanding research into cross-industry collaborations and intelligence-sharing frameworks could shed light on how coordinated efforts can enhance the collective resilience of organizations. Understanding the dynamics of collaboration, such as through shared platforms such as MISP or ThreatConnect, could contribute to more robust global strategies for combating cyber threats.

5 CONCLUSIONS

In this study, the effectiveness of the CKC Model for detecting and defending against cyber-attacks on companies and entities has been examined. Through a comprehensive review of specialized literature, it has been identified that the CKC model is widely recognized and utilized in the field of cybersecurity. This structured approach has proven valuable in identifying and neutralizing the stages of an attack cycle, enabling early detection and a more effective response to security incidents.

Research findings have shown that the CKC model is particularly useful for identifying and analyzing the tactics and techniques employed by attackers at each stage of the attack process. Similarly, differences in its effectiveness have been observed depending on the size and industry of organizations, suggesting the importance of adapting this methodology to the specificities of each context.

Despite the positive results, limitations have been identified related to access to academic literature and potential biases in the selection of articles. Therefore, organizations are recommended to consider adopting the CKC model as part of their cybersecurity strategies. Additionally, there is an urgent need to foster collaboration between cybersecurity experts, researchers, and professionals in the sector to generate new studies that expand knowledge about its effectiveness and adaptation to various environments. Overcoming these limitations will strengthen the understanding and application of the CKC model in the fight against cyber threats in today's digital world.

6 REFERENCES

[1] W. B. Glisson and R. Welland, "Web engineering security (WES) methodology," *Commun. Assoc. Inf. Syst*., vol. 34, pp. 1359–1396, 2014. https://doi.org/10.17705/1CAIS.03471

[2] D. Fischer, C. Sauerwein, M. Werchan, and D. Stelzer, "An exploratory study on the use of threat intelligence sharing platforms in Germany, Austria and Switzerland," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 2023, pp. 1–7. https://doi.org/10.1145/3600160.3600185

[3] R. Bold, H. Al-Khateeb, and N. Ersotelos, "Reducing false negatives in ransomware detection: A critical evaluation of machine learning algorithms," *Appl. Sci.,* vol. 12, no. 24, p. 12941, 2022. https://doi.org/10.3390/app122412941

[4] D. Ito *et al*., "Modeling attack activity for integrated analysis of threat information," *IEICE Trans. Inf. Syst*., vol. E101-D, no. 11, pp. 2658–2664, 2018. https://doi.org/10.1587/transinf.2017ICP0015

[5] A. Campazas-Vega, I. S. Crespo-Martínez, Á. M. Guerrero-Higueras, C. Álvarez-Aparicio, V. Matellán, and C. Fernández-Llamas, "Analyzing the influence of the sampling rate in the detection of malicious traffic on flow data," *Comput. Networks*, vol. 235, p. 109951, 2023. https://doi.org/10.1016/j.comnet.2023.109951

[6] W. Zeng and V. Germanos, "Modelling hybrid cyber kill chain," *CEUR Workshop Proc*., vol. 2424, pp. 143–159, 2019. https://ceur-ws.org/Vol-2424/paper10.pdf

[7] M. Allegretta, G. Siracusano, R. Gonzalez, and M. Gramaglia, "Are crowd-sourced CTI datasets ready for supporting anti-cybercrime intelligence?" *Comput. Networks*, vol. 234, p. 109920, 2023. https://doi.org/10.1016/j.comnet.2023.109920

[8] P. Zanna, P. Radcliffe, and D. Kumar, "Preventing attacks on wireless networks using SDN controlled OODA loops and cyber kill chains," *Sensors*, vol. 22, no. 23, p. 9481, 2022. https://doi.org/10.3390/s22239481

[9] A. Corallo, M. Lazoi, M. Lezzi, and P. Pontrandolfo, "Cybersecurity challenges for manufacturing systems 4.0: Assessment of the business impact level," *IEEE Trans. Eng. Manag.*, vol. 70, no. 11, pp. 3745–3765, 2023. https://doi.org/10.1109/TEM.2021.3084687

[10] A. Dimitriadis, E. Lontzetidis, B. Kulvatunyou, N. Ivezic, D. Gritzalis, and I. Mavridis, "Fronesis: Digital forensics-based early detection of ongoing cyber-attacks," *IEEE Access*, vol. 11, pp. 728–743, 2023. https://doi.org/10.1109/ACCESS.2022.3233404

[11] J. F. Andry *et al.*, "Data centre risk analysis using ISO 31000:2009 framework," *J. Phys. Conf. Ser.*, vol. 2394, no. 1, p. 012032, 2022. https://doi.org/10.1088/1742-6596/2394/1/012032

[12] B. Almutairi, "Secure mitigation and migration of virtual machines over hybrid cloud hypervisors infrastructure," *Int. J. Adv. Appl. Sci.*, vol. 8, no. 7, pp. 7–13, 2021. https://doi.org/10.21833/ijaas.2021.07.002

[13] R. Kour, A. Thaduri, and R. Karim, "Railway defender kill chain to predict and detect cyber-attacks," *J. Cyber Secur. Mobil.*, vol. 9, no. 1, pp. 47–90, 2020. https://doi.org/10.13052/jcsm2245-1439.912

[14] R. Hoffmann, J. Napiórkowski, T. Protasowicki, and J. Stanik, "Risk based approach in scope of cybersecurity threats and requirements," *Procedia Manuf.*, vol. 44, pp. 655–662, 2020. https://doi.org/10.1016/j.promfg.2020.02.243

[15] A. K. Pandey, A. Tripathi, A. Agrawal, R. Kumar, R. A. Khan, and M. Alenezi, "A framework for producing effective and efficient secure code through malware analysis," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 2, 2020. https://doi.org/10.14569/IJACSA.2020.0110263

[16] R. Kour, A. Thaduri, and R. Karim, "Predictive model for multistage cyber-attack simulation," *Int. J. Syst. Assur. Eng. Manag.*, vol. 11, pp. 600–613, 2020. https://doi.org/10.1007/s13198-020-00952-5

[17] H. Kim, H. J. Kwon, and K. K. Kim, "Modified cyber kill chain model for multimedia service environments," *Multimed. Tools Appl.*, vol. 78, pp. 3153–3170, 2019. https://doi.org/10.1007/s11042-018-5897-5

[18] L. M. Maruping, V. Venkatesh, J. Y. L. Thong, and X. Zhang, "A risk mitigation framework for information technology projects: A cultural contingency perspective," *J. Manag. Inf. Syst.*, vol. 36, no. 1, pp. 120–157, 2019. https://doi.org/10.1080/07421222.2018.1550555

[19] D. Kiwia, A. Dehghantanha, K. K. R. Choo, and J. Slaughter, "A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence," *J. Comput. Sci.*, vol. 27, pp. 394–409, 2018. https://doi.org/10.1016/j.jocs.2017.10.020

[20] H. I. Kure, S. Islam, and M. A. Razzaque, "An integrated cyber security risk management approach for a cyber-physical system," *Appl. Sci.*, vol. 8, no. 6, p. 898, 2018. https://doi.org/10.3390/app8060898

[21] I. Herwono and F. Ali El-Moussa, "Automated detection of the early stages of cyber kill chain," in *International Conference on Information Systems Security and Privacy*, vol. 1, 2018, pp. 182–189. https://doi.org/10.5220/0006543301820189

[22] E. Weintraub and Y. Cohen, "Defining network exposure metrics in security risk scoring models," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 4, 2018. https://doi.org/10.14569/IJACSA.2018.090456

[23] K. Park, S. Woo, D. Moon, and H. Choi, "Secure cyber deception architecture and decoy injection to mitigate the insider threat," *Symmetry*, vol. 10, no. 1, p. 14, 2018. https://doi.org/10.3390/sym10010014

[24] T. Kokkonen, "Architecture for the cyber security situational awareness system," in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems (ruSMART 2016, NEW2AN 2016)*, in Lect. Notes Comput. Sci., O. Galinina, S. Balandin, and Y. Koucheryavy, Eds., vol. 9870, Springer, Charm, pp. 294–302, 2016. https://doi.org/10.1007/978-3-319-46301-8_24

[25] T. Yadav and A. Mallari Rao, "Technical aspects of cyber kill chain," in *International Symposium, Security in Computing and Communications*, Kochi, India, 2015, pp. 438–452. https://doi.org/10.1007/978-3-319-22915-7

[26] P. Shedden, R. Scheepers, W. Smith, and A. Ahmad, "Incorporating a knowledge perspective into security risk assessments," *Vine*, vol. 41, no. 2, pp. 152–166, 2011. https://doi.org/10.1108/03055721111134790

[27] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K. K. R. Choo, and P. Burnap, "Impact and key challenges of insider threats on organizations and critical businesses," *Electron.*, vol. 9, no. 9, p. 1460, 2020. https://doi.org/10.3390/electronics9091460

[28] S. H. Rashid and W. D. Abdullah, "Enhanced website phishing detection based on the cyber kill chain and cloud computing," *Indones. J. Electr. Eng. Comput. Sci.,* vol. 32, no. 1, pp. 517–529, 2023. https://doi.org/10.11591/ijeecs.v32.i1.pp517-529

[29] J. L. Sandoval, L. Andrade-Arenas, D. H. Celis, and M. Cabanillas-Carbonell, "Enterprise information security risks: A systematic review of the literature," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 31, no. 3, pp. 1589–1604, 2023. https://doi.org/10.11591/ijeecs.v31.i3.pp1589-1604

[30] J. R. R. Kumar, D. G. Bhalke, S. Nikam, S. Chobe, S. Khidse, and K. Kale, "Evaluation of the extent and demanding roles of ethical hacking in cybersecurity," *J. Auton. Intell.*, vol. 7, no. 1, pp. 1–10, 2024. https://doi.org/10.32629/jai.v7i1.1246

[31] M. M. Yamin, M. Ullah, H. Ullah, B. Katt, M. Hijji, and K. Muhammad, "Mapping tools for open source intelligence with cyber kill chain for adversarial aware security," *Mathematics*, vol. 10, no. 12, p. 2054, 2022. https://doi.org/10.3390/math10122054

[32] F. Almeida, "Prospects of cybersecurity in smart cities," *Futur. Internet*, vol. 15, no. 9, p. 285, 2023. https://doi.org/10.3390/fi15090285

[33] W. Deng, W. Fan, Z. Li, C. Cui, X. Ji, and G. He, "Security of cyber-physical systems of chemical manufacturing industries based on blockchain," *Processes*, vol. 11, no. 9, p. 2707, 2023. https://doi.org/10.3390/pr11092707

[34] M. I. Alghamdi, "Survey on applications of deep learning and machine learning techniques for cyber security," *Int. J. Interact. Mob. Technol.*, vol. 14, no. 16, pp. 210–224, 2020. https://doi.org/10.3991/ijim.v14i16.16953

[35] M. M. Al-Nawashi, O. M. Al-hazaimeh, T. M. Nedal, N. Gharaibeh, W. A. Abu-Ain, and T. Abu-Ain, "Deep reinforcement learning-based framework for enhancing cybersecurity," *Int. J. Interact. Mob. Technol.*, vol. 19, no. 3, pp. 170–190, 2025. https://doi.org/10.3991/ijim.v19i03.50727

[36] I. Mustapha, Y. Vaicondam, A. Jahanzeb, B. A. Usmanovich, and S. H. B. Yusof, "Cybersecurity challenges and solutions in the fintech mobile app ecosystem," *Int. J. Interact. Mob. Technol.*, vol. 17, no. 22, pp. 100–116, 2023. https://doi.org/10.3991/ijim.v17i22.45261

7 AUTHORS

Junior E. Dávila-Huayhuapuma is with the Universidad Tecnológica del Perú, Lima, Perú.

Eduardo Vílchez-Roncal is with the Universidad Tecnológica del Perú, Lima, Perú.

Carlos A. Alvarado-Silva is with the Universidad Tecnológica del Perú, Lima, Perú (E-mail: c21629@utp.edu.pe).