A comparative analysis of cyber threat intelligence models

Roman Odarchenko[1,†], Alla Pinchuk[1,*,†], Oleh Polihenko[1,†] and Anatolii Skurativskyi[1,†]

[1] *National Aviation University, Liubomyra Huzara Ave. 1, Kyiv, 03058, Ukraine*

Abstract

Cyber Threat Intelligence (CTI) plays a crucial role in modern cybersecurity by providing actionable insights into attacker behavior, motives, and tactics. As the threat landscape evolves, so too do CTI models, each with its own strengths and weaknesses. This article presents a comparative analysis of various CTI models, such as Diamond Model, Extended Diamond Model, Cyber Kill Chain, Unified Cyber Kill Chain and MITRE ATT&CK Model, exploring their core functionalities, underlying methodologies, and suitability for different use cases. By understanding the nuances of each model, security professionals can make informed decisions about which CTI approach best suits their organizational needs.

Keywords

cyber threat intelligence, CTI models, models analysis

1. Introduction

In the current conditions of development and widespread use of information and communication technologies (ICT), fundamentally new substances have been formed: the information society, information space, and cyberspace, which now play an important role in many areas of our lives. However, despite its many advantages, this has caused many problems related to the protection of ICT systems that suffer from cyberattacks on a daily basis.

The ever-expanding digital landscape has ushered in a new era of cyber threats, characterized by sophisticated attacks, targeted campaigns, and persistent adversaries. To effectively combat these threats, organizations require a comprehensive understanding of the attacker landscape. This is where Cyber Threat Intelligence (CTI) comes into play. CTI is the process of collecting, processing, and analyzing information about both existing and emerging threats that may target your organization. It serves as a proactive security measure, preventing data breaches and reducing the financial costs of incident recovery. CTI includes information related to cyber threats and threat actors, using a variety of sources for identification. The process includes research, analysis, and modeling to prevent and detect attacks [1]. The general concept of CTI is information sharing. In the absence of adequate information about threats, organizations will not be able to respond effectively.

CTI requires a contextual perspective and focuses on analyzing the results and effectiveness of the information contained in the intelligence. This may include past, present, and future tactics, techniques and procedures (TTPs). In addition, the relationships between each identified piece of information can be linked and mapped to create a visual representation. Based on [2], CTI is divided into four subtypes, as shown in Figure 1. Description of all these subtypes is below:

CH&CMiGIN'24: Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, January 24–27, 2024, Kyiv, Ukraine

[*] Corresponding author.

[†] These authors contributed equally.

odarchenko.r.s@ukr.net (R. Odarchenko); pinchuk.ad87@gmail.com (A. Pinchuk); o.poligenko@ukr.net (O. Polihenko); 7993538@stud.kai.edu.ua (A. Skurativskyi)

0000-0002-7130-1375 (R. Odarchenko); 0000-0003-3567-0445 (A. Pinchuk); 0000-0002-2427-4976 (O. Polihenko); 0009-0000-0566-2394 (A. Skurativskyi)

© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR-WS.org/Vol-3925/paper01.pdf

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

- **Strategic**: it provides a high-level perspective on threat intelligence, considering financial impact, attack trends, and global implications. It focuses on long-term usability of gathered intelligence. In this context, analysts examine attack patterns across industries, changes in TTPs over time, malware usage, and data breaches. Strategic CTI informs executive decisions and guides long-term security planning. On the other hand, subtype CTI delves beyond technical risks, considering the motivations behind attacks. It takes into account who or which organization is behind the attacks, their objectives, and why they target specific entities. Subtype CTI serves as an early warning system for anticipated threats, aiding organizations in proactively establishing defences based on current attack trends, without necessarily revealing specific methods or codes.
- **Tactical**: focuses on understanding threat actors' methods of operation. It equips responders and defenders with knowledge to prepare alarms, defences, and investigations against the latest threats. Sources for tactical CTI include white papers, technical press, and interactions with other organizations and peers. Specifically, tactical CTI provides detailed information about attackers. This encompasses mapping out threat actor TTPs, defining their goals, and understanding their technical capabilities. Armed with this intelligence, organizations can proactively fine-tune their mitigation tactics and even simulate attacks to identify vulnerabilities in their security infrastructure.
- **Technical**: it focuses on specific threat indicators, such as Indicators of Compromise (IoCs), relevant to SOC Staff. Aligned with operational intelligence, technical CTI helps identify signs of ongoing attacks. By leveraging threat intelligence platforms with AI, organizations can automatically scan for known indicators, including phishing email content, malicious IP addresses, and specific malware implementations. SOC and incident response teams can swiftly respond to this information, preventing potential damage to the organization. Analysts gather information about the attacker's command and control (C2) infrastructure, tools, malware, and other technical resources used against the organization.
- **Operational**: it focuses on specific threats against an organization, considering threat actor motivations, vulnerability exploitation, past and current malicious activity, and the impact of cyberattacks on confidentiality, integrity, and availability. It helps assess an organization's resilience against cyber threats. Operational CTI provides specialized information about attacker identities, motivations, and methods. Automation through a cyber threat intelligence platform enhances data collection efficiency [2–5].

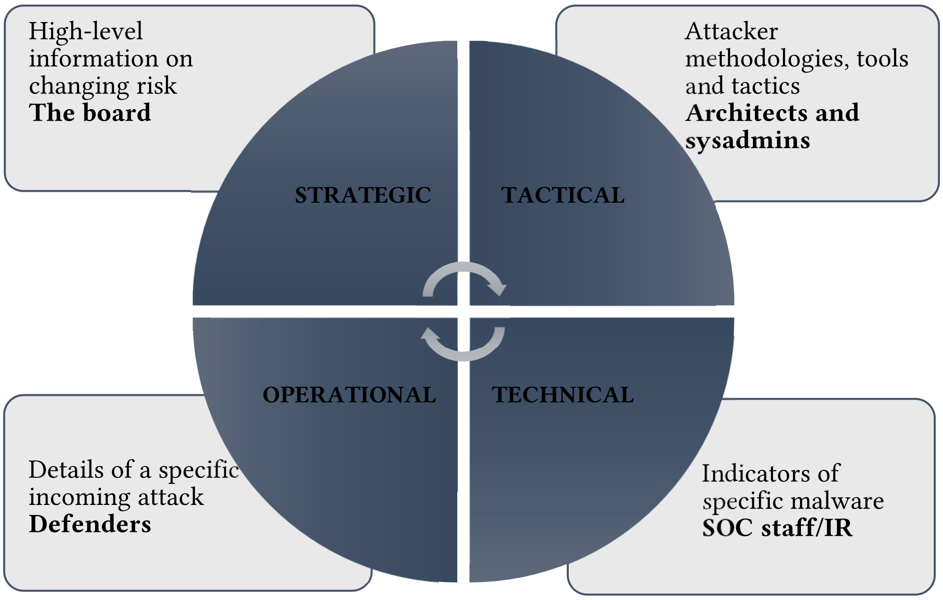

High-level information on changing risk
The board
Attacker methodologies, tools and tactics
Architects and sysadmins
STRATEGIC
TACTICAL
OPERATIONAL
TECHNICAL
Details of a specific incoming attack
Defenders
Indicators of specific malware
SOC staff/IR

Figure 1: CTI subtypes.

For every subtype, there are also different methods for gathering information, such as OSINT (Open-Source Intelligence), CSINT (Closed Source Intelligence), HUMINT (Human Intelligence) and TECHINT (Technical Intelligence).

CTI models enable organizations to effectively organize and analyze CTI data, gaining a comprehensive understanding of the evolving threat landscape. To achieve all CTI goals, different Cyber Threat Intelligence models are used. Each CTI model offers unique perspectives and methodologies to analyze, understand, and mitigate these threats. At the same time, each model has advantages and disadvantages that cyber security specialists in organizations need to take into account.

There are a lot of CTI models available, and research was conducted regarding their use in CTI systems. In [6], the usage, pros and cons of such models as the F2T2EA model, the Cyber Kill Chain model, the Diamond model of intrusion analysis, and the Q model were discussed. According to [7, 8], there are three models that stand above all other existence models: Cyber Kill Chain, MITRE ATT&CK, and Diamond; they use different approaches, but all of them are very useful in CTI. In [9], the most effective models of cybersecurity organizations were discussed.

Thus, the aim of this article is to analyze the most common Cyber Threat Intelligence models and provide full comparison regarding their usage in CTI systems.

2. The Diamond Model and the Extended Diamond Model

2.1. The Diamond Model

The Diamond model represents a new concept for analyzing intrusions developed by cybersecurity analysts. This model establishes the basic "atomic element" of any intrusion activity or cyber incident consists of four main functions: adversary, infrastructure, capability, and victim that are shown on Figure 2. Because of the shape formed by the relationships between all these elements, this model is named as a Diamond [10].

When an event is detected, the vertices of the model are filled in automatically or with the help of analysts.

The vertices are connected by edges and highlight the natural connections between functions, such as adversary-victim, adversary-infrastructure, victim-infrastructure and victim-capability [11]. As analysts follow the edges and vertices, they discover more information about the attacker's operations and identify new capabilities, infrastructure, and victims.

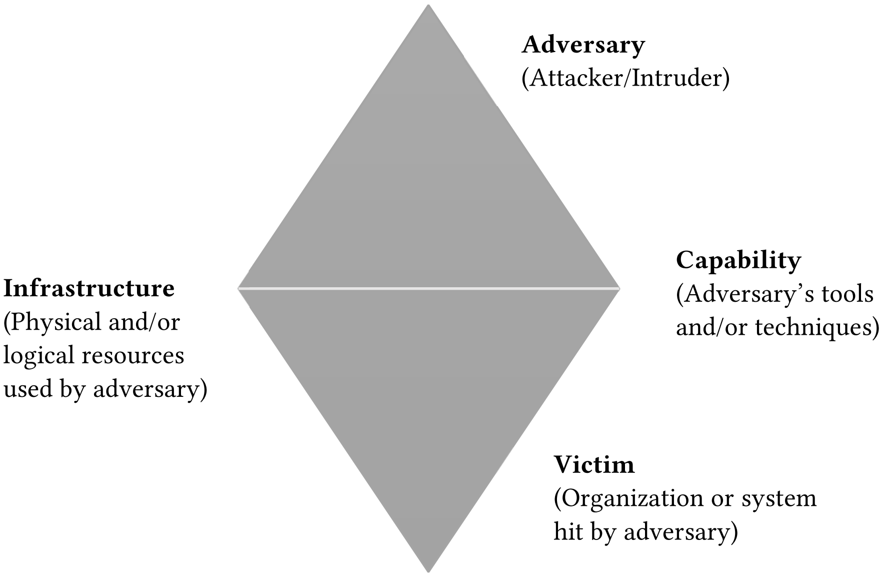


Figure 2: The Diamond Model.

The Diamond model includes the next meta-features [10]:

- **timestamp**: date and time intrusion event occurred;
- **phase**: which event, in the chain of events, is represented by this particular model;
- **result**: outcome of intrusion (e.g., success, failure, or unknown; or confidentiality compromised, integrity compromised, and/or availability compromised);
- **direction**: how event moved through network or host (e.g., Victim-to-Infrastructure, Adversary-to-Infrastructure, Bidirectional);
- **methodology**: category of event (e.g., spear phishing, port scan);
- **resources**: elements required for intrusion (e.g., particular software, hardware, knowledge, funds, facilities, access).

According to [12], this model establishes scientific principles and applies formal methods to intrusion analysis, including measurement, testing, and comparison, providing a comprehensive methodology for documenting, synthesizing, and correlating processes during the intrusion investigator's activities.

This scientific approach and simplicity results in improved analytical efficiency, productivity, and accuracy. After all, the Diamond Model provides the ability to integrate real-time vulnerability intelligence to protect networks, automate and correlate events, classify them by confidence level in adversarial campaigns, predict adversarial operations in planning, and develop cost reduction strategies.

2.2. The Extended Diamond Model

The Extended Diamond Model has some additional features that complement the original model and make it more informative for analysts. New features for Extended Diamond Model are socio-political meta-features to determine the relationship between the adversary and victim as well as technology meta-features for infrastructure and capabilities [13]. The scheme of model is shown on Figure 3.

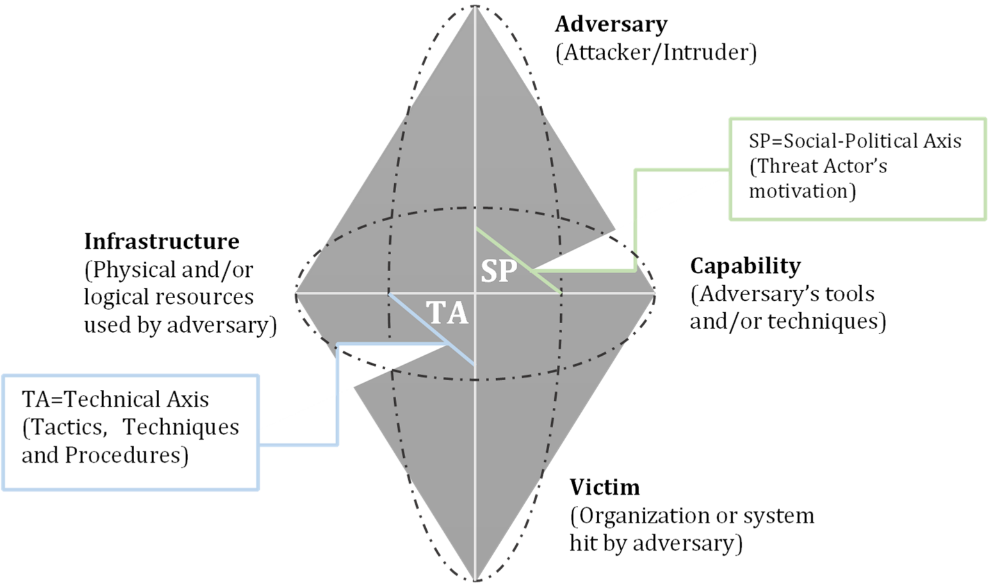


Figure 3: The Extended Diamond Model.

Considering both versions of this model, it is worth adding a few key aspects. First of all, it makes it simple for analysts to switch between different intelligence pieces, which either helps to reveal intelligence blind spots or complete the picture while acquiring intelligence. Tracking enemies, capabilities, infrastructure, and victims over time is the model's primary goal. An activity thread that links trends in attackers, TPPs, and infrastructure across assaults against several victims is used to display this activity. By outlining possible future directions that threat actors might go, the activity thread helps defenders and responders approach security pro-actively rather than reactively.

The diamond model's capacity to create activity groups and activity-attack graphs is another essential feature. Activity groups are collections of shared identifying behaviors, such as a specific APT activity or a typical attack path that threat actors use to indicate a particular kind of attack. Activity-attack graphs are visual depictions of real attacks that take place at various points along the cyber death chain in the threat landscape. In order to create scenarios that a company would encounter, this enables CTI analysts to monitor ongoing activity in the threat landscape and correlate the MITRE ATT&CK TPPs to the cyber death chain. Security teams may create targeted threat hunt scenarios and make sure their security stack defends against assaults encountered in the field by using these attack graphs [14]. An example of such a graph is discussed in [10, 15].

3. The Cyber Kill Chain and the Unified Cyber Kill Chain

3.1. The Cyber Kill Chain Model

The Cyber Kill Chain (CKC) Model was developed in 2011 by the US company Lockheed Martin and mainly focused on Advanced Persistent Threat (APT) attacks [16]. Focusing on APT attacks, create a strong impact on the CTI field. Generally, this model represents a series of steps that an attacker must execute to reach his or her final objective based on the F2T2EA (Find, Fix, Track, Target, Engage, Assess) concept [17]. The scheme of this model is shown on Figure 4. Explanation of each step is in [18, 19]. The variants of this model are shown in [20].

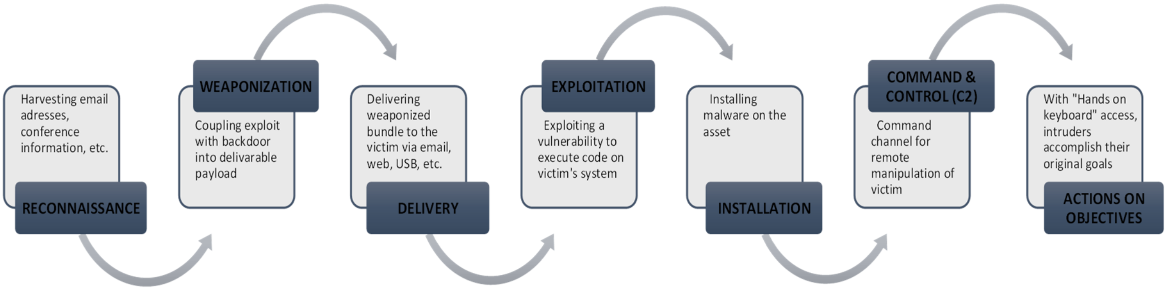

Harvesting email adresses, conference information, etc.
RECONNAISSANCE
WEAPONIZATION
Coupling exploit with backdoor into delivarable payload
Delivering weaponized bundle to the victim via email, web, USB, etc.
DELIVERY
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
Installing malware on the asset
INSTALLATION
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
With "Hands on keyboard" access, intruders accomplish their original goals
ACTIONS ON OBJECTIVES

Figure 4: The Cyber Kill Chain Model.

From the other side, here we cannot see the defender's part. If we present time scale correctly and name some steps according to defender side, the whole attack can be divided in the next phases:

- Preparation (Phase 1 Reconnaissance, Phase 2 Arming);
- Incident (Phase 3 Delivery, Phase 4 Intrusion, Phase 5 Installation);
- Active Intrusion (Phase 6 C2, Phase 7 Action).

This model also has some problems. Firstly, it should be noticed that the flaw in this model lies in its oversimplified portrayal of cyber-attacks as tidy and linear processes, which diverges from the messier reality. Moreover, Cyber Kill Chain tends to focus solely on the immediate actor behind a cyber-attack, disregarding the underlying motives or any potential insider collaboration. To enhance the model’s effectiveness, it’s crucial to supplement it with knowledge about the attack’s sponsor, drawing insights from real-world espionage cases [6].

Despite its limitations, this model remains valuable for organizations seeking to fortify their defenses by addressing vulnerabilities at each link in the chain, provided they have access to high-quality intelligence on the adversary’s actions throughout the process.

3.2. The Unified Kill Chain Model

The Cyber Kill Chain Model has been improved, the new approach was created and named Unified Kill Chain (UKC) Model. The main idea of this model is to combine two existing models: the Lockheed Martin' Cyber Kill Chain and the MITRE ATT&CK for Enterprise [21].

The MITRE ATT&CK Framework offers a comprehensive inventory of adversary tactics and techniques, while the Lockheed Martin Kill Chain offers a methodical view of an attacker's intrusion stages. By merging these frameworks, the Unified Kill Chain allows enterprises to evaluate their defenses from two different perspectives [22]:

- strategically, taking into account the stages of an attack;
- tactically, emphasizing particular attacker actions.

This combination enables organizations to assess their security posture holistically and adjust their defensive strategies as necessary.

The Unified Kill Chain consists of eighteen phases, or strategies, that a cyberattack could go through. Phases may be skipped, repeated, or executed out of order by any given attack. The scheme of this model is shown on Figure 5.

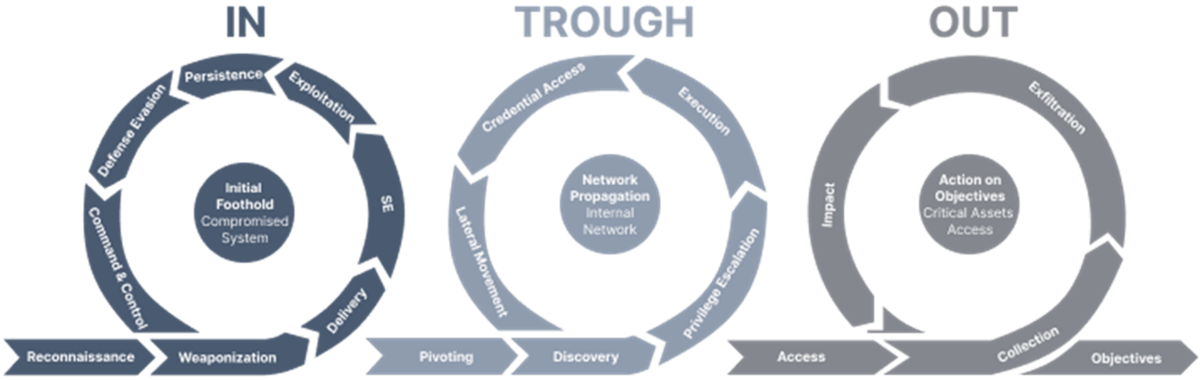


Figure 5: The Unified Kill Chain Model.

It is possible to combine several tactical phases of an attack to accomplish intermediate goals, like getting a first foothold in a targeted network, breaking into it to increase your level of access, and taking action against important assets.

All typical cyberattack activities, from the initial reconnaissance conducted by external attackers to the successful accomplishment of the attack's ultimate goals beyond the organizational perimeter, can be modeled using the Unified Kill Chain. The Unified Kill Chain relies on the expertise of industry leaders such as Lockheed Martin' Cyber Kill Chain and MITRE's ATT&CK for Enterprise model in order to cover such a wide range.

4. The MITRE ATT&CK model

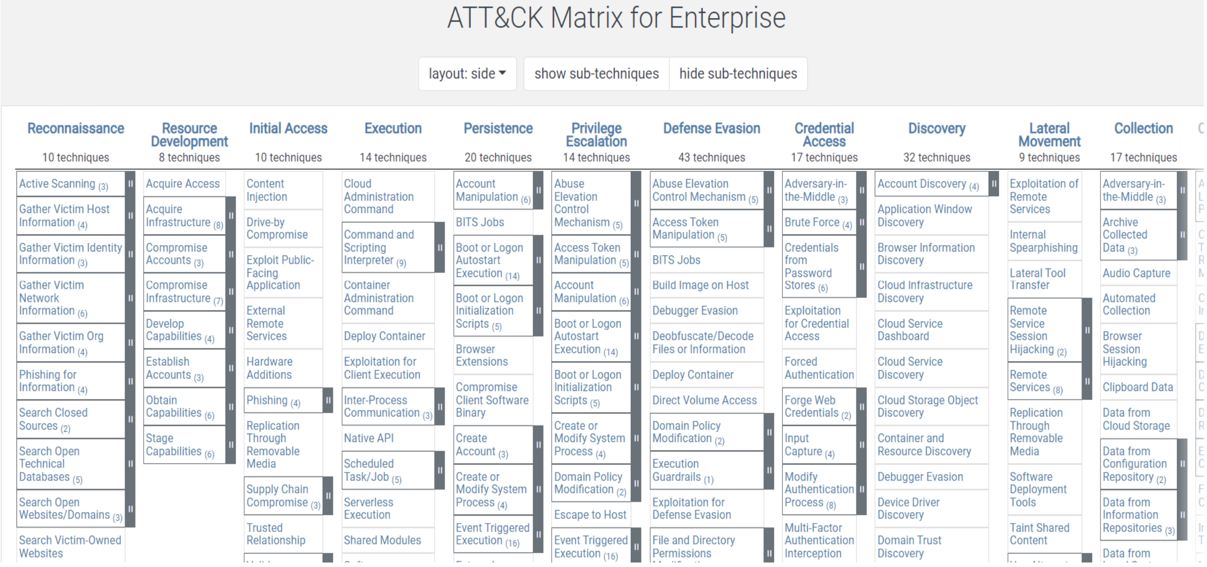
The MITRE Corporation developed the framework, data matrices, and assessment model known as MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) to assist organizations in assessing their security readiness and identifying weak points in their defenses [23]. Most of all, it is a hub for exchanging knowledge and information about cyberattacks with an emphasis on the development and execution of TTPs, where tactics stand for the reasons behind the actions an attacker takes to accomplish their goal, techniques for how the attacker carries out the actions, and procedures for the specific steps involved in putting the techniques into practice [7].

The adversary's "technical objectives" are divided into 14 tactics categories within the framework: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defence Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and

Control, Exfiltration and Impact [24]. Each category includes techniques and sub-techniques (Figure 6).

It can be said that the matrix is basically a historical reference of what techniques and methods were popular among cybercriminals in the past, as well as a fresh look at the cyberthreat model through the prism of techniques that hackers are actively using now [25, 26]. But it is worth adding that in MITRE ATT&CK, one technique can be repeated in several columns of the matrix [27]. This is because attackers may have different goals, but may use the same means to achieve them.

The MITRE ATT&CK Matrix is looked at by security researchers from around the world. For analysts, it's a good source to help structure information about current attack techniques. Knowing how real APT groups operate allows you to formulate hypotheses for proactive threat hunting.


ATT&CK Matrix for Enterprise

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Escape to Host	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion		Data from Information Repositories (3)
Search Victim-Owned Websites			Shared Modules			Execution Guardrails (1)		Device Driver Discovery		Data from
						Exploitation for Defense Evasion		Domain Trust Discovery		
						File and Directory Permissions				

Figure 6: The MITRE ATT&CK matrix.

Despite of advantages of this model, it also has some disadvantages:

- It's huge and complicated.
- There is a lot of data to be processed, and many organizations have not automated much of that data in terms of mapping it to their security infrastructure or to other data they have in their system.
- There are various attack patterns that are constantly evolving, making it impractical to detect and map them against your security infrastructure.

5. Comparison amongst different models

The Diamond Model and the Extended Diamond Model have different approaches than other models. In this case, we can compare these models regarding their focuses, granularities, and applications. These characteristics provide a full understanding of each model and their use in CTI (Table 1).

Despite the fact that CKC, UKC, and MITRE ATT&CK are providing a lot of useful information for incident response, attribution of a cyberattack to a threat actor is a complicated procedure that the Diamond Model and the Extended Diamond Model excel at through all their features (both non-meta and meta). In fact, attribution should not be solely based on the analysis of an adversary's use of TTPs alone.

By combining models that have different approaches, security teams will be able to get a complete picture of cyber threats, how to protect their organization, and how to respond to incidents more effectively [28–31].

Table 1
Models' Comparison

Characteristic	Diamond/ Extended Diamond	Cyber Kill Chain / Unified Kill Chain	MITRE ATT&CK
Focus	Model emphasizes attacker motivations and capabilities	Model emphasizes attack stages	Model emphasizes attack stages, techniques, sub-techniques, TTPs, etc.
Granularity	Model offers a broader perspective	Model is more specific	Model is more specific
Application	Model is useful for threat intelligence and threat hunting	Model is focused on incident response	Model is useful for understanding the behavior of threat actors via documenting the TTPs used in previous attacks.
Maintenance	Users of the Diamond Model will need to feed it themselves	In case of UKC, model uses MITRE ATT&CK matrix	MITRE ATT&CK is maintained directly by MITRE and indirectly by the cybersecurity community
Covered attack's steps	Not in scope	CKC – 7; UKC – 18	14
Value	Presence of a deep understanding of the infrastructure and capabilities of both victim and adversary	By combing UKC and MITRE ATT&CK, model provides full understanding of each attack step	Presence of a study of the tactics, methods and tools used

6. Conclusions

The cyber threat landscape is complex and constantly changing. Each CTI model offers unique perspectives and methodologies for analyzing, understanding, and mitigating these threats.

The Diamond Model/Extended Diamond Model is used only to analyze cyberattacks (intrusions), to formalize them in order to answer the questions "who", "why" and "how" implemented the cyberattack, provides IoCs of cyberattacks for further examination, but this model does not reflect the stages of attacks.

Models such as CKC, UKC, and MITRE ATT&CK take into account the stages of cyber attacks, with UKC covering more stages than the other two models. At the same time, MITRE ATT&CK serves as a broad knowledge base of intruder's TTPs and provides a full understanding of threat actor behavior. However, these models do not answer the question of what to do when an attack is successful, nor do they pay attention to intrusion prevention.

Combining multiple models or frameworks often results in a more holistic and effective approach to cybersecurity, enabling organizations to proactively defend against a variety of cyber threats. Continuously evolving and adapting these models is essential to staying ahead in the ongoing battle against cyber adversaries.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] Cyber threat intelligence, 2018. URL: https://iitd.com.ua/en/rozvidka-kiberzagroz-cti/.

[2] T. Punz, Cyber threat intelligence, 2018. URL: https://www.securnite.com/index.php/onepress_service/cyber-threat-intelligence/.

[3] L. Taggart, Why does strategic threat intelligence matter?, 2023. URL: https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/why-does-strategic-threat-intelligence-matter.html.

[4] A. Funkhouser, Understanding cyber threat intelligence, 2022. URL: https://www.netskope.com/blog/understanding-cyber-threat-intelligence.

[5] What is cyber threat intelligence?, 2022. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-cyber-threat-intelligence.

[6] M. Sahrom, S. R. Selamat, A. Ariffin, Y. Robiah, An enhancement of cyber threat intelligence framework, Journal of Advanced Research in Dynamical and Control Systems 10 (2018) 96–104.

[7] A. Sánchez del Monte, L. Hernández-Álvarez, Analysis of cyber-intelligence frameworks for AI data processing, Appl. Sci. 13.16 (2023) 9328. doi: 10.3390/app13169328.

[8] N. Naik, P. Jenkins, P. Grace, J. Song, Comparing attack models for IT systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK framework and diamond model, in: Proceedings of International Symposium on Systems Engineering (ISSE), IEEE, Vienna, Austria, 2022, pp. 1–7. doi: 10.1109/isse54508.2022.10005490.

[9] O. Volot, Information and cybernetic security of modern enterprise: Provision and modeling, Central Ukr. Sci. Bull. Econ. Sci. 3(36) (2019) 238–247. doi: 10.32515/2663-1636.2018.3(36).238-247.

[10] C. Warner, Diamond model in cyber threat intelligence, 2021. URL: https://warnerchad.medium.com/diamond-model-for-cti-5aba5ba5585.

[11] D. Tidmarsh, What is the Diamond Model of Intrusion Analysis in cybersecurity, 2023. URL: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/diamond-model-intrusion-analysis.

[12] A. Zhylin, M. Hudyncev, M. Litvinov, Functional model of cybersecurity situation center, Collect. Inf. Technol. Secur. 6.2 (2018) 51–67. doi: 10.20535/2411-1031.2018.6.2.153490.

[13] A. Hearts, Diamond Model of Intrusion Analysis, 2024. URL: https://medium.com/@agapehearts/diamond-model-of-intrusion-analysis-81af3ee1baeb.

[14] Strategies for Gathering and Contextualizing Cyber Threat Intelligence. URL: https://www.netskope.com/blog/strategies-for-gathering-and-contextualizing-cyber-threat-intelligence.

[15] S. Caltagirone, A. Pendergast, C. Betz, The diamond model of intrusion analysis, Threat Connect 298(0704) (2013) 1–61.

[16] E. M. Hutchins, M. J. Cloppert, R. M. Amin, Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, Leading Issues in Information Warfare & Security Research 1(1) (2011) 80.

[17] C. D. Means, E. Darling, J. Perron, Applying Cognitive Work Analysis to Time Critical Targeting Functionality, Center For Air Force C2 Systems, Bedford, MA (2004).

[18] I. Tarnowski, How to use cyber kill chain model to build cybersecurity?, European Journal of Higher Education IT (2017). URL: https://www.eunis.org/download/TNC2017/TNC17-IreneuszTarnowski-cybersecurity.pdf.

[19] T. Yadav, A.M. Rao, Technical aspects of cyber kill chain. In: J. Abawajy, S. Mukherjea, S. Thampi, A. Ruiz-Martínez (Eds.), Security in Computing and Communications. SSCC 2015, volume 536 of Communications in Computer and Information Science, Springer, Cham, 2015, pp. 438–452. doi: 10.1007/978-3-319-22915-7_40.

[20] J. van den Berg, The unified kill chain, 2017. URL: https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain-Thesis.pdf.

[21] P. Pols, J. van den Berg, The unified kill chain, CSA Thesis, Hague, 1–104 (2017).

[22] J. Garrett, The Unified Kill Chain: Your Tool for Actively Evaluating Your Cyber Defenses, 2022. URL: https://www.opkalla.com/articles/the-unified-kill-chain-your-tool-for-actively-evaluating-your-cyber-defenses.

[23] Understanding Cyber Kill Chain, MITRE ATT&CK Framework and Unified Kill Chain, 2023. URL: https://medium.com/@wintersoldiers/understanding-cyber-kill-chain-mitre-att-ck-framework-and-unified-kill-chain-f306ceca19be.

[24] MITRE ATT&CK, 2023. URL: https://attack.mitre.org.

[25] Y. Averyanova, et al., UAS cyber security hazards analysis and approach to qualitative assessment, In: S. Shukla, A. Unal, J. Varghese Kureethara, D.K. Mishra, D.S. Han (Eds.), Data science and security, volume 290 of Lecture Notes in Networks and Systems, Springer, Singapore, 2021, pp. 258–265. doi: 10.1007/978-981-16-4486-3_28.

[26] M. Zaliskyi, et al., Heteroskedasticity analysis during operational data processing of radio electronic systems, in: S. Shukla, A. Unal, J. Varghese Kureethara, D.K. Mishra, D.S. Han (Eds.), Data science and security, volume 290 of Lecture Notes in Networks and Systems, Springer, Singapore, 2021, pp. 168–175. doi: 10.1007/978-981-16-4486-3_18.

[27] R. S. Odarchenko, S. O. Gnatyuk, T. O. Zhmurko, O. P. Tkalich, Improved method of routing in UAV network, in: Proceedings of International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD), IEEE, Kyiv, Ukraine, 2015, pp. 294–297. doi: 10.1109/APUAVD.2015.7346624.

[28] M. Zaliskyi, R. Odarchenko, S. Gnatyuk, Y. Petrova, A. Chaplits, Method of traffic monitoring for DDoS attacks detection in e-health systems and networks, CEUR Workshop Proceedings 2255 (2018) 193–204. URL: https://ceur-ws.org/Vol-2255/paper18.pdf.

[29] V. Kharchenko, I. Chyrka, Detection of airplanes on the ground using YOLO neural network, in: Proceedings of 17th International Conference on Mathematical Methods in Electromagnetic Theory (MMET), IEEE, Kyiv, Ukraine, 2018, pp. 294–297. doi: 10.1109/MMET.2018.8460392.

[30] O. Sushchenko, et al., Airborne sensor for measuring components of terrestrial magnetic field, in: Proceedings of IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO), IEEE, Kyiv, Ukraine, 2022, pp. 687–691. doi: 10.1109/ELNANO54667.2022.9926760.

[31] O. Solomentsev, M. Zaliskyi, O. Kozhokhina and T. Herasymenko, Efficiency of data processing for UAV operation system, in: Proceedings of 4th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD), IEEEб Kiev, Ukraine, 2017, pp. 27–31. doi: 10.1109/APUAVD.2017.8308769.