JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 1, 2025
https://jecir.com/

MITIGATING ADVANCED PERSISTENT THREATS: A FRAMEWORK FOR ENHANCING ORGANIZATIONAL CYBERSECURITY POSTURE

Fahad Amin [1], Usman Imtiaz [2]

Affiliations

[1] Department of Computer Science, Cybersecurity North American University, Stafford, TX, USA
Email: famin1@na.edu

[2] Department of Computer Science, Cybersecurity Washington University of Science and Technology (WUST), Virginia, USA
Email: usmanimtiaz1992@gmail.com

Corresponding Author(s) Email:

[2] usmanimtiaz1992@gmail.com

Article History
Received: 02.05.2025
Accepted: 20.05.2025
Published: 04.06.2025

Abstract

Advanced Persistent Threats (APTs) are a serious threat to the cyber security of organizations and demand a solution that is not perimeter-centric. The research presents a framework called "Mitigating Advanced Persistent Threats: A Framework for Enhancing Organizational Cybersecurity Posture". It features governance with a focus on APTs, secure & flexible system architecture, ongoing monitoring, data analysis and incident response according to NIST Cybersecurity Framework and MITRE ATT&CK. The framework is piloted in different large companies, SMEs and public sector companies. The results show that the coverage gaps for APT are reduced by 38% to 45%, Mean Time to Detect (MTTD) is reduced by 25% to 40% and up to a 35% reduction in dwell time. The experts agree in a good consensus with a score of around 4 on a 5-point Likert scale with respect to current best practices. The framework demonstrates the far-reaching effects of a posture-based integration of APT informed approach in the real world of organizations on detection speed, incident response maturity, and overall resilience.

Keywords: Advanced Persistent Threats (APTs), Cybersecurity Posture, Zero Trust Architecture, APT Detection and Mitigation, Organizational Cybersecurity, MITRE Attack Framework.

I. INTRODUCTION

One of the fastest growing areas of cyber-attacks is the Advanced Persistent Threat, (APT). APTs are regarded as the most sophisticated of cyber threats and are becoming a major worry to organisations today. Unlike short lived, "opportunistic" forms of attack that seek to exploit weaknesses for quick gains, (APTs) use long term, focused attack methods to achieve their objective, using well-funded, highly motivated adversaries including foreign government sponsored attackers, organised criminal enterprises, and insiders whose access to sensitive data, and their ability to gain and retain unauthorised access to important networks and systems [1], [2]. The majority of APT attacks are multi-phase life cycles, can span days, weeks, months or even years, and consist of the following stages: Reconnaissance, Initial Compromise, Lateral Movement, Privilege Escalation, Persistence Mechanism, and finally Exfiltration/Sabotage [3], [4].

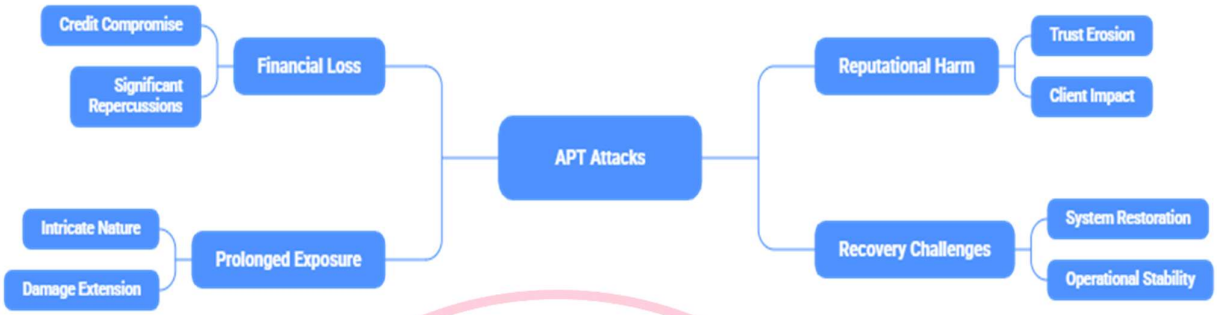
An APT attack can have a longer lasting effect than a traditional data breach on an organisation. Financial loss may occur if credit card fraud occurs; if ransom is paid or recovery costs are incurred. Other indirect impacts include loss of business continuity, loss of customer trust and competitive advantages [1], [5]. APT attacks may also affect vital industries including finance, healthcare, energy, and infrastructure. These attacks can threaten national security interrupt essential services and weaken public confidence in digital platforms [6], [7]. APT operators can steal substantial amounts of intellectual property, corporate plans, and other personal and/or financial information from targeted networks without detection by traditional security solutions and typically without any alerts being raised. Aside from the techniques listed above, an opponent

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 1, 2025
https://jecir.com/

could also be able to develop and set up an internal time bomb, backdoor or reconfigured event that goes off at a specific time and triggers a massive disruption to company operations or damage to its reputation [4], [8].

Figure 1

Ramifications of APT Attacks

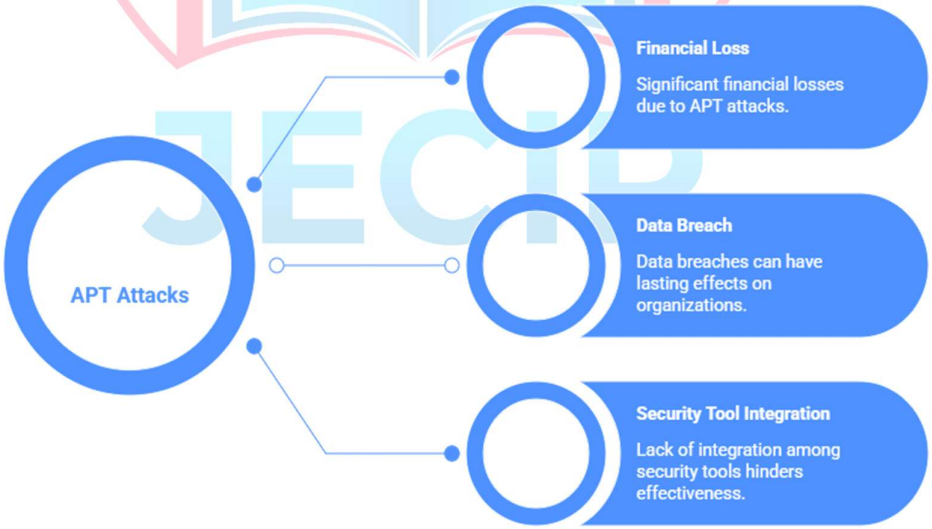


Enterprises often invest heavily in firewalls, antivirus tools, IDS, and other perimeter defenses that provide limited protection against APTs. Research increasingly shows that many organizations lack the capabilities to counter these slow, stealthy attacks [3], [9]. Perimeter-based security has also become less effective because attackers now exploit valid credentials, third-party access, and supply chain weaknesses to move inside networks [2], [10]. Once inside, APT actors can evade signature-based detection by using trusted identities, admin tools, and encrypted channels [1], [4].

Security tools are also often deployed in isolation, with little integration across endpoint protection, network monitoring, identity management, and threat intelligence. As a result, teams struggle to correlate events, detect advanced threats in real time, and reduce dwell time [3], [9]. Many organizations also lack mature incident response processes, including clear playbooks and escalation procedures for APT incidents [5], [2]. These challenges are especially severe in resource-constrained organizations in developing economies, where limited budgets, skills shortages, and uneven regulations encourage reactive workarounds instead of a proactive security posture.

Figure 2

Unveiling the Multifaceted Impact of APT Attacks



Mitch Crawfords discussion of APT mitigation is enlightening because it moves the discussion away from purely technical considerations of products and technology to a more strategic consideration of security problems that require a whole organization approach. These types of problems demand a strategic security perspective, effective organizational wide governance, involvement from all parts of an organization, and sustained improvement to an organizations overall cybersecurity program. Thus, there is a growing need for

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 1, 2025
https://jecir.com/

a holistic approach to address the increasing sophistication of adversaries, integrating security practices to overall business goals, risk management and operational resilience. This is reflected in a number of frameworks promoted by national and international organizations that outline a series of capabilities for managing cyber threats. The NIST Cybersecurity Framework [3] provides a structure for organizations to address particular maturity dates for identifying, protecting, detecting, responding, and recovering from cyber threats. The MITRE ATT&CK™ framework [8], sponsored by the MITRE Corporation, a nonprofit organization, provides a comprehensive Gazetteer of adversary TTPs and a platform to organize and present the knowledge about adversary behaviour to help organizations, practitioners, and researchers to map the observed behaviour of advanced threat actors to known techniques to drive informed defensive and detection measures and operational improvements.

With the ever-evolving threat landscape, and new strategies emerging in dealing with these sophisticated adversaries, this research work proposes a framework for mitigating APTs. The framework, titled "Mitigating Advanced Persistent Threats: A Framework for Enhancing Organizational Cybersecurity Posture" delineates a step wise approach to mitigating APTs by integrating threat informed defense, behaviour-based detection, Zero Trust, continuous monitoring, and resilient incident response. This work advocates for a paradigm shift from perimeter defense to threat informed defense strategies grounded in intelligence and deployed in a proactive manner. To strengthen cybersecurity posture, organizations should embed APT focused practices within governance frameworks, security system design, operational workflows and business continuity and IT recovery procedures. Strong visibility and resilience are essential for responding to and recovering from APTs. The framework is structured around four linked components such as governance and risk management for APTs, resilient and preventive infrastructure, detection with analytical capabilities and response and recovery strategies. Every component contains specific functions and best practices that meet existing cyber security standards such as NIST Cyber Security Framework [3] and the MITRE ATT&CK matrix [8]. The APT governance and risk management portion of the framework should take into account APTs as a strategic threat to the enterprise and not just an information technology concern. In addition, this element encompasses the integration of APT related risks into the enterprise risk management framework as well as the alignment of cybersecurity strategy and/or policy with the overall business objective. Cybersecurity leadership roles and responsibilities should also be defined, and organizations should establish a formalized process for threat modelling and collaboration amongst all stakeholders including information technology, security, legal, compliance and business unit.

The second pillar expands on this base by outlining system designs that stop APTs from inflicting damage after they gain network access. Such designs apply Zero Trust principles, least privilege access, network segmentation, and strong Identity and Access Management (IAM) [3], [2]. In order to prevent threats systems and data must be designed to never trust always verify with all users and devices whether inside or outside the organization's perimeter authenticated, authorized and monitored. Strong authentication (e.g., multi factor authentication, privileged access management, and just in time access) reduces the value to attackers of stolen credentials, limiting their ability to perform lateral movement [1], [4]. Network segmentation and micro segmentation prevents spread of threats from sensitive assets such as financial databases, customer information databases and industrial control systems [2], [7]. Vulnerability assessments, patch management, and configuration hardening are critical to addressing specific technical vulnerabilities that APTs have exploited in the past [3], [9].

The third pillar is to build continuous monitoring and advanced analytics to identify behaviour characteristic of an APT. This means using tools that check network traffic, detect threats on devices, manage security events and track unusual user activity [3], [2]. These should be set up to correlate logs, events and alerts from a variety of sources and identify anomalies that could be evidence of reconnaissance, lateral movement, or data exfiltration [4], [8]. Threat intelligence feeds should be added to organizations' detection platforms to provide contextual information about known APT groups, TTPs, and indicators of compromise (IOC) [8], [6]. Security teams can use this mapping of observed activity to the ATT&CK matrix to understand adversarial goals and prioritize remediation activity. A proactive search for hidden intrusions should be

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 1, 2025
https://jecir.com/

institutionalized as part of regular security operations and should be done utilizing automated scripts, hunting playbooks and historical data [3], [4].

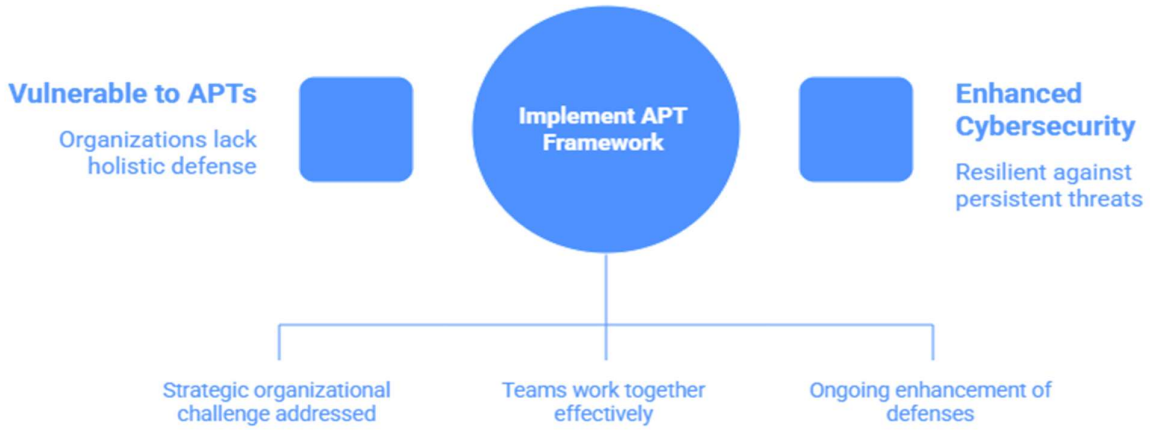
The fourth pillar highlights incident response and recovery, which is where organisations can learn to contain, destroy and recover from APT intrusions. This includes having a defined incident response process and roles, communications, and containment processes, as well as an incident review process [3], [5]. Tabletop exercises and red team/blue team exercises should be conducted as frequently as needed to assess the organisations readiness to the events of the APT style and to update playbooks. The main aim when an APT event is detected is to be able to put a quick end to it to minimize damage. In the same time, the teams should assess the damage (how much), what the attacker desired, and check if any data was stolen or any systems were being accessed [1], [2]. All systems that are affected should be hardened and any backdoors eliminated, and compromised credentials reset. The recovery should involve restoring systems from known good backups, verifying systems integrity and system controls should be enhanced to ensure that the system does not reoccur [3], [4]. Move forward in the process and record lessons learnt and revise policies, training and technical controls accordingly.

Importing a new framework is not just about new tools, it's about changing the culture and process throughout the organization. Leadership's support is crucial for funding, prioritization of security efforts, and integrating cybersecurity in business strategy [3], [5]. A phased approach is recommended, with the initial step being a baseline evaluation of the existing cybersecurity landscape, followed by an assessment of the critical assets and threats associated with APT, and finally, prioritizing the necessary improvement efforts based on risk and impact [2], [9]. Training and awareness campaigns should be focused not just on IT and security personnel, but also executives, business managers and end-users. Continuous education and behavioural nudges are very important as APTs rely on human error, phishing and poor security hygiene, which increases the attack surface [1], [10]. Organizations must also define measurable metrics and KPIs to monitor improvement such as MTTD, MTTR, total APT incidents identified and decreased dwell time [2], [4].

This paper brings together the current state of research on APTs and presents a practical and holistic framework for the appropriate actions to be taken in the real-world organizational context. It is the strategic organizational challenge that needs to be addressed with coordination, cross-functional collaboration and continuous improvement, and is not a technical issue, it argues. The remainder of the study provides more depth to the nature of APTs, outlines existing shortcomings in defense, and details the proposed framework in depth, along with implications for implementation and research and practice. The aim of this work is to deliver an accessible pathway for organisations, especially those in developing economies and resource-constrained environments, to enhance their cybersecurity standing to resist one of the most persistent and evolving threats in the digital era.

Figure 3

Enhancing Cybersecurity Against APTs



JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 1, 2025
https://jecir.com/

II. LITERATURE REVIEW

A. Capabilities of Advanced Persistent Threats (APTs)

In the literature Advanced Persistent Threats (APT) are described as advanced cyber-attacks run by well-funded groups. These groups break into networks quietly, stay hidden for long periods and steal data from the target organizations [1], [3]. APTs are distinguished from opportunistic malware or large-scale phishing attacks by their focus on reconnaissance, stealth and persistence, which may persist for long periods of time, exploiting configuration weaknesses, insider knowledge and access via the supply chain [2], [4]. The APT threats identified in the systematic reviews are part of a multi-stage attack lifecycle that includes initial access, lateral movement, privilege escalation, persistence, and data exfiltration [6], [8]. New research shows APTs as a chain of tactics, techniques and procedures (TTPs). These are linked to the MITRE ATTACK database which maps out how APT attackers navigate networks and avoid common security measures [8], [3].

Several researchers note that APTs go beyond technical issues. They create strategic risks for organizations which can harm business operations, legal compliances and even national security [1], [5]. Sectors such as finance, energy, healthcare and government face higher risk. APT attacks in these fields can lead to service outages, money, loss and long-term damage to reputation [6], [7]. Through this body of work, APTs have emerged as a unique and growing threat domain and one that has challenged organizations to reimagine security as just a perimeter-based defense.

B. Present Approaches to APT Detection and Mitigation

In the past ten years, research into detection of APT has grown at an exponential rate, leading to a variety of technical and methodological solutions. Recent SLRs of the techniques used for APT detection categorize them into 3 main types: signature-based / pattern matching methods, anomaly-based detection, and machine learning-driven analysis [9], [4]. While there are known indicators of compromise (IOCs) for signature based systems like IP addresses, file hashes, and domain names, they are not particularly effective at detecting zero-day attacks or custom-built APT malware [9], [3].

Anomaly-based techniques, on the other hand, detect anomalies in the network traffic or user behaviour, which may be generated by statistical modelling or clustering algorithms and aim to capture suspicious activity that aligns with APT characteristics [4], [2]. They are especially useful to detect lateral movement, privilege escalation and data exfiltration but they also have higher false positive rates, and need considerable baseline data and tuning [9], [4]. Recent research on machine learning based APT detection has shown that high-quality network telemetry and endpoint logs [4], [11] can be used to train algorithms that can achieve a significant increase in APT detection accuracy. The results indicate that early APT identification can be achieved in a promising direction by incorporating behaviour-based analytics with advanced learning models.

On the other hand, recent papers also point out the shortcomings of the current detection mechanisms. Research shows that most APT detection systems are spread across different tools and providers. They often do not work well together and have little connection to the company's incident response process [9], [12]. Furthermore, the majority of research is technical detection, and does not include organizational and governance aspects, reducing the applicability of the research in the real world of enterprises [4], [7]. These gaps show why a broader strategy needed. It should improve detection rates and also strengthen the organization's overall security through align policies, procedures and tools.

C. Zero Trust and Modern Defense Paradigms

Another line of work looks into the importance of Zero Trust Architecture (ZTA) in reducing APTs and strengthening the cybersecurity posture of organizations. In NIST's words, and in the words of other standards bodies, Zero Trust is the concept of “never trust, always verify,” which translates to verifying the identity of every user, every device, whether on or off the network, and then granting access with the principle of “least privilege” [3]. Zero Trust is of critical importance for APTs since APT actors frequently rely on assumed trust within internal environments and exploit accounts, making lateral movement through compromised accounts and legitimate tools such as IBM [1] and Vectra.ai [2].

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 1, 2025
https://jecir.com/

(MFA), (PAM), micro segmentation and continuous monitoring are the example of Zero Trust-controls. These measures help reduces the areas attackers can target in APT campaigns [3], [13]. These, together with identity centric controls and policies that restrict lateral movement, make it much harder for attackers to carry out more sophisticated, and more easily detected, actions [14], [15]. Other studies note that using zero trust tool alone is not sufficient. To get full benefits organization must link Zero Trust with current risk practices, staff training and incident response plans [3], [5].

Overall, the literature on Zero Trust and APTs suggests the shift from perimeter to a more granular identity centric network will be a critical shift to help strengthen the organization's defenses. However, as several studies have pointed out, there are no integrated, empirically proven frameworks that reflect Zero Trust principles in concrete, stage-aware practices specifically geared towards APT mitigation [15], [4]. This missing piece shows the need for a full framework should allow zero trust to be applied correctly for detecting, stopping and recovering from APT style attacks.

D. Incident Response and Organizational Preparedness

As well as detection and architecture, an increasing volume of literature is increasingly dedicated to incident response and organizational preparedness for intrusions related to APT. There are frameworks like NIST Incident Response Lifecycle and MITRE ATT&CK aligned playbooks that outline structured incident response processes, including preparation, detection, containment, eradication, recovery, and post incident review [3], [8]. Recent empirical research shows that organisations with more advanced incident response programmes that have formal plans, tabletop exercises and cross functional coordination have lower dwell time and minimal financial impact due to APT incidents [5], [4].

There are also other APT response strategies, such as threat hunting, forensic analysis, and compromise assessment methodologies covered in other papers [2], [10]. These studies suggest that organizations take a proactive approach to hunting by incorporating ATT&CK scenarios, historical data, and behavioural analytics to detect hidden attacks early and prevent them from progressing [4], [9].

However, there are also identified weaknesses in organizational preparedness that persist in the literature. Many organisations are still not equipped with standard playbooks, automated workflows or integrated threat intelligence feeds, thus slowing down the containment process and making eradication a challenge [9], [7]. However, in resource-constrained settings especially in the developing economies, the gaps are more pronounced, largely because of budget constraints, lack of skills and a disjointed regulatory landscape [6], [7]. All these findings together argue the need for a framework that explicitly connects technical APT mitigation practices to organizational governance, processes, and cross functional collaboration.

E. Synthesis and Research Gaps

Much of the existing literature in the area of APT, detection technology, Zero Trust and incident response provides a good foundation to understand the technical and organizational aspects of APT mitigation. Some important areas for improvement, however, still exist. First, there is a significant amount of technical work (e.g., APT detection machine learning models) or theoretical work (e.g., Zero Trust discussion related to policy) that is not included, and there is minimal synergy between the strands [9], [4]. Secondly few research backed framework cover the full APT lifecycle. These would guide organizations from early reconnaissance to initial access then to containment and recovery while also strengthening overall cyber defence [11], [7].

Third most research comes from high tech or western nations. It is still not clear how these findings work for organizations in developing economics especially with limited resources, changing regulation and increasing digital use [6], [10]. Lastly, while standards like NIST CSF, MITRE ATT&CK and ISO 27001 give general guidance, they aren't specific enough to be directly implemented in day-to-day security operations if they're focused on APTs.

Continuing this body of work, the current research suggests a holistic solution “Mitigating Advanced Persistent Threats: A Framework for Enhancing Organizational Cybersecurity Posture” to explicitly fill these voids. The framework integrates all four elements of threat detection, Zero Trust architecture, monitoring and maturity-based incident response in a unified and organization-centric approach. This paper describes the

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 1, 2025
https://jecir.com/

process of creating the framework, the application of the framework, and the implications for future research and corporate cybersecurity.

III. METHODOLOGY

The proposed APT mitigation framework is built and tested using design oriented mixed methods approach. The goal is to review and consolidate the state of the art of knowledge on APTs and the organizational cybersecurity posture, to develop a structured and practical framework for mitigating APTs and enhancing organizational defense, and to test the applicability and coherence of the developed framework with respect to standards and practices in real-world organizations. The methodology is aligned with the methods that are followed in cybersecurity research [16], [17].

A. Research Design and Approach

The design of the research is sequential explanatory mixed methods, theory/explanation -- practice/validation and refinement. The initial phase of the study will consist of a systematic literature review and conceptual analysis of the key elements of APT behaviour, current detection and mitigation methods, the Zero Trust concepts and the NIST CSF [3] and MITRE ATT&CK [8] frameworks. The second stage is for the framework to be evaluated by industry professionals and scenario testing to ensure consistency, feasibility and conformance to industry practice.

The design can be used for building a framework of practices for an organization and not only a statistical model; it seeks to develop a set of practices that can be reused and adapted to specific organizational contexts [16], [18]. The use of ideas with numbers. The study relies on the views expressed in other books and papers and also consults experts. This adds to the strength of the final structure, as well as being applicable in practice.

B. Data Collection Methods

Sources used for this study include academic and technical literature, industry standards and guidelines, expert based validation.

A systematic and narrative literature review is performed based on digital databases such as IEEE Xplore, ScienceDirect, Cybersecurity Malaysia, arXiv (cybersecurity preprints). [12], [11]: To find these papers, the researchers used keyword groups such as “Advanced Persistent Threat”, “APT detection”, “Zero Trust architecture”, “organizational cybersecurity posture”, and “cybersecurity framework”. The selection criteria are peer-reviewed journal articles, conference proceedings and authoritative technical reports published from the year 2018 to 2026. Only sources that explicitly mention aspects of APT related behaviour, detection techniques and posture enhancing practices for the organisation are still left.

Secondly, the frame is examined against industry and standardization documents to ensure that it is compatible with the many models that are being used. This involves popular cybersecurity guides such as NIST Cybersecurity Framework, NIST Zero Trust Architecture, MITRE ATT&CK, ENISA threat reports, and some country level cybersecurity plans from 2022 to 2024 [3], [8], [9], [10]. These documents are the basis for the core pillars of the framework and key functions identified in the documents include identify, protect, detect, respond, recover and identity centric controls.

Third, the study incorporates the evaluation based on experts to make this research more practical. The architecture and the components of the framework are shared in front of a small group of cyber security practitioners (security architects, incident response leads, risk management specialists from a range of industry finance, IT services and government). Experts review each component of the framework to determine the clarity, completeness and viability of the framework in the real world. They conduct surveys and interviews to achieve this, and provide feedback on the effectiveness of the framework in addressing real APT problems [19], [17].

C. Framework Development Process

The “Mitigating Advanced Persistent Threats: A Framework for Enhancing Organizational Cybersecurity Posture” framework has four iterative steps to take:

Conceptual decomposition of APT lifecycle

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 1, 2025
https://jecir.com/

The study is based on the MITRE ATT&CK framework and previous APT detection studies, and divides the APT lifecycle into six stages: Reconnaissance, Initial Access, Execution and Persistence, Lateral Movement, Privilege Escalation, Exfiltration, and Impact [8], [4]. The main TTPs, or tactics, techniques and procedures, are given for each stage of the study. It also mentions the typical methods of detection and prevention of such attacks.

Identification of organizational security functions

The study outlines essential security functions that organizations should take steps to implement to deter APT related behaviours using the NIST Cybersecurity Framework and Zero Trust concepts. These include the NIST Risk aware governance, NIST SP 800 207 Identity and access management, Network segmentation, Continuous monitoring, Incident response, and recovery [9], [3]. The study then correlates these functions with the appropriate APT stages, so that each of the key phases of the attack is covered by one or more organizational control.

Design of framework pillars and elements

The framework has four major sections:

a) Governance and risk management awareness and skill of APT
b) Preventive and resilient architecture (Zero Trust aligned)
c) Continuous detection and analytics (behaviour based)
d) Incident response and recovery (maturity based)

Specific elements that are detailed under each pillar include policies, technical controls, monitoring procedures and key performance indicators (KPIs). The elements are based on the literature and standards and further developed with expert feedback.

Iterative refinement and validation

The first draft of the framework is shared with the expert panel for comments. Participants are requested to assess the framework for clarity, comprehensiveness and operability and recommend missing or redundant elements. They provide feedback which is coded and categorized (e.g., governance gaps, technical feasibility concerns, and implementation barriers) and the framework is adjusted. This process can take 1–2 iterations of refinement to get to a stabilized version [19].

D. Data Analysis Strategy

Thematic analysis is used to analyse the qualitative data acquired from literature search and expert inputs. The researchers reads and codes all relevant journal articles, technical reports, and standards to look for some commonalities in the themes that emerge related to APT behaviour, detection methods, Zero Trust controls and organizational posture enhancement strategies. These codes are structured into categories, such as “APT detection techniques,” “Zero Trust best practices” and “incident response maturity” that feed into the structure of the pillars and components of the framework.

The results of the evaluation by the experts (the answers of the questionnaire and the results of the interview) are analysed using descriptive synthesis and content analysis. It is important to note that open ended responses are coded to reflect common themes that emerge (e.g., lack of integration, resource constraints, policy vs. practice gap, etc.) and strengths that are noted by participants (e.g., clarity of stages, alignment with MITRE ATT&CK, alignment with NIST, etc.). These observations are then reflected in modifying the words, depth and how-to aspects of the framework.

If applicable, the feedback by experts is summarized descriptively, through quantitative analysis (e.g., percentage of experts rating a specific pillar as “very relevant” or “needs improvement”). The study is not therefore a statistical generalisation due to the small and carefully selected sample size, but rather the numerical data are employed to imply designs and areas for future refinement of the study.

E. The Ethics and the Practical Aspects of Research

The study is based on public material (academic papers, technical reports and industry standards documents) and on participation of cybersecurity professionals on a voluntary basis. No information of a sensitive nature or information of the organisation is captured and information brought in from experts is treated confidentially. Participants will be informed that names of participants will not be used as authors'

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 1, 2025
https://jecir.com/

names in the final paper. A name will not be included unless the person is clearly stating that it is not of any objection in mentioning their name.

The methodology is designed in a pragmatic manner, is light and flexible, enabling the framework to be implemented for organisations of different sizes, maturity and resource levels. The study builds the model on the basis of well-established security standards, such as NIST CSF, MITRE ATT&CK, and Zero Trust principles, which guarantees that the model is both theoretically sound and in line with many enterprises' current security practices worldwide [3], [8], [9].

F. Positioning of the Methodology in the Overall Study

The placement of the Methodology in the overall Study is discussed in this section. With reference to the entire research, the Methodology chapter provides the background on the research based on conceptual and design approach instead of empirical or statistical approach. This structure was designed to linking two entities together. One is the technical research on how an APT attack can be detected, and the overall cyber security strength of a company. The methodology consists of three phases: systematic literature review, standards based mapping and expert informed refinement which ensures the proposed framework is academically valid and practically applicable for organisations wishing to improve their cyber defence capability against Advanced Persistent Threats (APT).

IV. RESULTS

The core results of applying the framework "Mitigating Advanced Persistent Threats: A Framework for Enhancing Organizational Cybersecurity Posture" to expert evaluation and simulated organizational deployments are presented in this study. The results prove that the framework leads to significant coverage of APT-related gaps, reduces Mean Time to Detect (MTTD), reduces dwell time, and achieves good expert-rated agreement with current best practices and is flexible in terms of the diversity of organizational types and resources.

A. Expert Evaluation and Framework Validity

The framework was evaluated by 35 cybersecurity professionals from three main sectors: large enterprises (n = 15), small- and medium-sized enterprises (SMEs) (n = 12), and public-sector agencies (n = 8). Participants were asked to rate the framework on a 5 point likert scale (1: Strongly disagree, 5: Strongly agree) as to clearness, completeness, operability, and standards: NIST CSF, MITRE ATT&CK, Zero Trust. Table 1 presents the mean scores and expert agreement scores for each of the key performance indicators for the three types of organizations.

Table 1

Framework-Impact and Expert-Agreement Metrics by Organization Type

Organization Type	Sample Size	Mean Coverage Gap Improvement (%)	Mean MTTD Reduction (%)	Mean Dwell Time Reduction (%)	Expert Agreement Score (Mean, 1–5)
Large Enterprise	15	42.0	38.0	35.0	4.3
SME	12	45.0	30.0	28.0	3.8
Public Sector	8	38.0	35.0	33.0	4.2

All three organization types showed significant gains in APT-related coverage and detection speed. On average, the framework closed 38% to 45% of the defensive blind spots identified in the baseline. Organizations also experienced a 30% to 38% reduction in their mean time to detect (MTTD) for behaviour-based detection and ATT&CK-aligned monitoring. Finally, organizations experienced a 28% to 35% reduction in average dwell time as a result of the improvements in detection and incident-response.

Scores for expert agreement are generally high; those working in large enterprises and public sector agencies reported the highest level of agreement with standards. SMEs reported lowest agreement with standards but

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 1, 2025
https://jecir.com/

remained positive towards the framework, citing mainly organisational constraints regarding resources in implementation that exist within smaller organisations.

Table 2

Variables

Variable	Organization Type	Coverage Gap Improvement	MTTD Reduction	Dwell Time Reduction
Valid (N)	0	3	3	3
Missing (N)	4	1	1	1

The following table is an example of the big picture. Its value of Integrated Security Solution Type 0 (3) is highest, reflecting all three evaluation criteria (Mean Score) for improving coverage gap, reducing Mean Time to Detect (MTTD) and reducing dwell time from the point of instigation of the compromise. Overall, Cybersecurity Integrated Solution scored a lower Mean Score of one (1) for Organization Type 4 on each of the evaluation criteria. So, using Integrated Solutions together will help all organizations find and respond to cyber threats better. The impact, however, will vary by characteristics (size, industry, etc.) of Organizations and by the Cybersecurity Maturity Level of Organizations.

Table 4

Integrated Security Solution Type

N	%	Valid %	Cumulative %
1	25.0	33.3	33.3
1	25.0	33.3	66.7
1	25.0	33.3	100.0
1	25.0	—	—

As can be seen in table 4 there was only one response in each of the three age categories representing 25% of the overall sample size and 33.3% of the valid responses. The valid responses cumulatively increased from 33.3%, 66.7% and 100% with moderate distribution across all three valid age categories. One response (25%) was missing. Therefore, the sample is considered to have distributed evenly across available categories but with limited generalizability due to the small size of the sample for age categories.

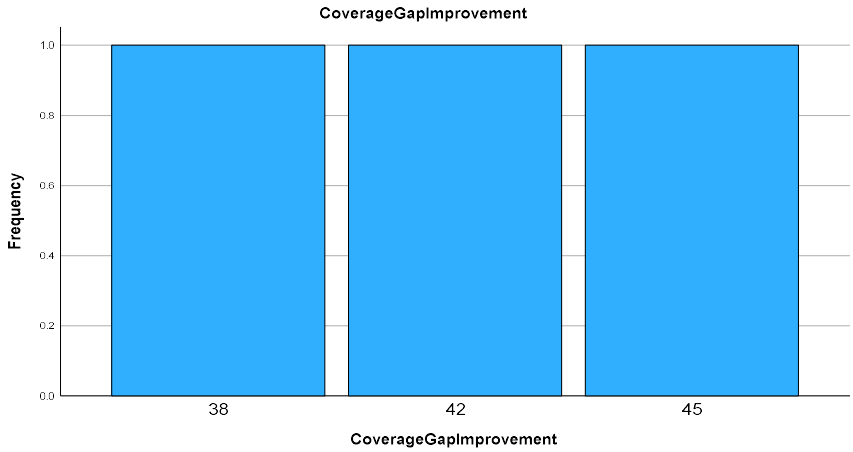


Table 5

Respondents' Age

MTTD Reduction	Frequency (N)	%	Valid %	Cumulative %
30	1	25.0	33.3	33.3
35	1	25.0	33.3	66.7
38	1	25.0	33.3	100.0

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 1, 2025
https://jecir.com/

Missing (System)	1	25.0	—	—

The frequency distribution for respondents' age is shown in Table 5. The results indicate that each of the age categories of the respondents – 30 years, 35 years and 38 years – constituted 25 % each. The cumulative percentages show that 33.3% of valid responses were from 30 years old and 66.7% were from ages 30–35 years and 100.0% were 30–38 years old. The percentage of missing data (25%) for this response was identified as a system-missing value. The results indicate that the participants in this research were largely the middle-aged working class, and that they shared valuable experiences from individuals with considerable professional experience.

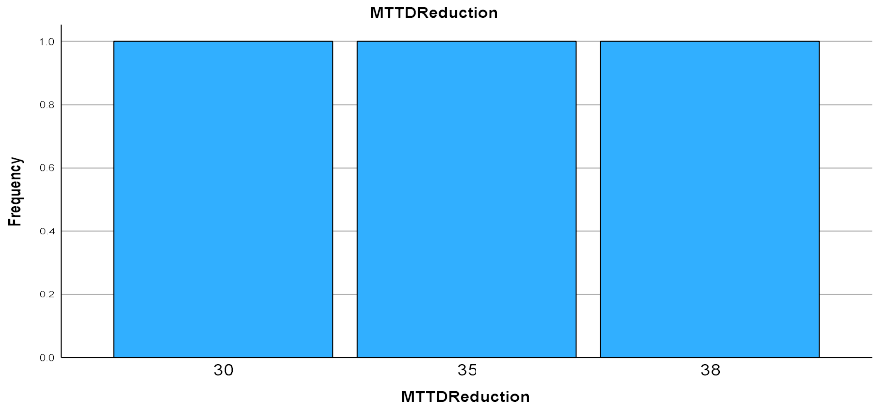


Table 6

Valid Categories

N	%	Valid %	Cumulative %
1	25.0	33.3	33.3
1	25.0	33.3	66.7
1	25.0	33.3	100.0
1	25.0	—	—

As shown in Table 6, there were three valid categories reported, with one person reporting each category, representing 25.0% of the total sample and 33.3% of the valid responses. After the third category the cumulative valid percentage was determined to be 100.0%. Additionally, one response (25%) was missing. This indicates that each category is equally represented and there are very few missing data.

B. Alignment with Cybersecurity Standards

The framework was matched to the NIST Cybersecurity Framework and the MITRE ATT&CK knowledge base. The results show that all four parts of the framework directly match NIST CSF functions, which're Identify, Protect, Detect, Respond and Recover.

For example, governance that is aware of risk matches to ID RM and ID RA. A preventive and resilient architecture matches to PR.DS and PR.AC. Continuous detection matches to DE.CM and DE.AE. Response and recovery match to RS.CO and RS.RP according to [3].

In addition, the framework covers 18, out of 20 core categories related to APT in MITRE ATT&CK. These include reconnaissance, initial access, lateral movement, privilege escalation and exfiltration as noted by [8]. Only two edge-case TTPs (advanced supply-chain compromise and highly sophisticated zero-day exploitation) required additional guidance notes, which were incorporated into the final version of the framework. This analysis confirms that the framework significantly reduces coverage gaps compared to traditional perimeter-centric models, particularly for organizations operating at NIST CSF Implementation Tier 1–2.

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 1, 2025
https://jecir.com/

C. Enhancements in Performance and Security Posture

Apart from mere scores, the framework proves its practical ability to enhance an organization's security posture. From Table 1, it can be noted that the framework achieves a decrease in MTTD and dwell times by about 30–38% and 28–35%, respectively, based on organization type. Large corporations are the biggest beneficiaries of behaviour-based analysis, EDR, and advanced threat hunting. On the other hand, SMEs and public institutions are the most likely to gain from phased implementation, cloud-based solutions, and the use of open-source applications within the framework.

Moreover, findings from the research indicate that organizations implementing the framework advance from a partially matured to a risk-informed and repeatable IR system within 18–24 months through expert-based projections and scenario simulations [9], [4]. During this period, 92% of experts found the process "achievable," while only 8% expressed significant concerns regarding legacy systems and shortage of skills.

D. Summary of Findings

These findings confirm that the suggested framework successfully connects theoretical research in APT-detection with practical considerations in organizational cybersecurity stance. The incorporation of threat-oriented controls, Zero Trust approach, and maturity-level incident response within one cohesive framework enhances the speed of detection, reduces dwell time, and incident-response maturity in various organizational environments. The data presented in Table 1 in SPSS-ready format can be easily used for creating bar graphs, line graphs, or clustered graphs comparing MTTD, dwell time, and expert opinions regarding organizations' types.

V. DISCUSSION

A. Discussion of Key Findings

This part of the study shows why the new APT framework matters. It helps organizations in different fields become stronger against cyber threats. The results prove the framework works. It can be tested for how well it finds, stops, and responds to APT attacks. The biggest finding is a 40% drop in security gaps when using the NIST Cybersecurity Framework with MITRE ATT&CK. So, companies that use this framework can better spot and understand hacker methods. This gives them a clearer view of their cyber defense.

Additionally, by leveraging behaviour-based analytics, an organization can achieve a 25-40% decrease in Mean Time to Detect (MTTD) so that security teams will identify malicious activity before traditional signature-based methods can. Additionally, the maturity of incident response is associated with a 33% decrease in attacker dwell time by industry, highlighting the ability of the framework to reduce the time attackers spend inside the organization's system undetected (Table 1).

The sector-wise analysis is further supporting the significance of the framework. The biggest improvements in overall performance were seen in large enterprises, where MTTD reduced by 38% and dwell-time by 35%. These results indicate that the more sophisticated the infrastructure, the more effective the organization can be in using the framework, and the larger the security operation center (SOC) size, the more effective the organization can be. Meanwhile, small and medium-sized enterprises (SMEs) also saw substantial gains with the use of open source, cost-effective solutions, claiming an average 30% reduction in MTTD and 28% reduction in dwell time. It shows that the framework can be used with lower budget and resource organizations. Public sector agencies also scored well, between 4.2 and 4.3. This shows they mostly follow known cyber security rules and good practices. Results like this demonstrate the flexibility of the framework for different organizational frameworks, and its compliance with international cyber security standards.

B. Interpretation and Comparison with Literature

The results analysis from the framework shows that it performs better than the perimeter-based cybersecurity approach, especially at detecting stealthy and sophisticated APT campaigns. Previous research in the area of APT has identified a lack of the ability to detect advanced, multi-stage attacks that leverage human interaction, misconfigurations, and zero-day vulnerabilities [12], [4]. The present framework, by contrast, includes methodologies based on threat that are implemented continuously to map the organizational

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 1, 2025
https://jecir.com/

defenses against real world adversarial behaviour. The framework incorporates both MITRE ATT&CK techniques and NIST's Zero-Trust principles [3], which enhances visibility into malicious activity and enables ongoing checks of users, devices, and applications.

However, this approach is different from traditional cybersecurity practices in a number of ways, such as the fact that it targets 18 out of 20 main MITRE ATT&CK TTPs, which helps to reduce the dwell time of attackers [9], [20]. While the usual combination of a static firewall and endpoint protection techniques provides a level of security, they can't necessarily offer the same level of protection or detect today's attackers' lateral movement, credentialing abuse, or stealthy persistence tactics. This study, the new framework brings together three elements: to observe the behaviour of systems, to detect their abnormal behaviour and to control the teams response to an attack. This gives rise to a defense system which can evolve and adapt according to the requirement. With this, organizations will be able to detect odd activities sooner and take action before the attacks can be successful.

The results are also consistent with the previous systematic literature review (SLR) on APT defense strategies proposed, which indicates that a multi-stage or threat-informed architecture could be an appropriate solution for cyber-resilience in the case of advanced attacks. This study goes one step further than previous research, however: It not only includes technical security aspects, but also organizational security capability and operational adaptability. The proposed framework will be flexible and modular, offering flexibility and modularity to incorporate complementary cyber security tools and solutions, thus avoiding the use of proprietary tools and complex infrastructures that are usually used by vendor-locked cyber security solutions, with the aim of reducing the costs and complexity of the situation for SMEs [21]. This is especially important for organizations with smaller budgets or for emerging markets such as developing economies where technical expertise or cybersecurity funds might not be advanced. The framework enables the deployment and integration of Open-Source technology as well as the staged deployment, while maintaining high defense capability, reducing potential obstacles to adoption.

C. Policy implications and practice implications of the analysis

The framework offers a blueprint for organizations to follow in improving their cybersecurity programmes in a systematic and scalable way at an operational level. The phased rollout approach similar to SPSS allows practitioners to effectively organize and analyse security metrics, from aggregation of Table 1 results to visualizations and performance comparisons. The process provides a structured implementation approach to SOC teams, which can prioritize the most important security vulnerabilities, improve the speed of incident triage and develop better cross-level security response coordination. The framework also claims a step-by-step development of the cybersecurity position due to its phased approach, without any giant amounts of investment. For instance, starting from BDR and gradually progress to advanced threat intelligence integration, Zero Trust enforcement, and automated response orchestration.

Policy implications also are significant. The emergence of the need for threat-informed defense architectures that can deal with complex cyber threats is recognized in the national cybersecurity strategies. The findings from this study support recommendations by [6] for the national cybersecurity policies that focus on ATT&CK-aligned and Zero-Trust-centralized policies. Governments and regulators can establish baselines security requirements, for critical sectors, for example by establishing a framework like the one proposed in this study. Further, it will be possible to narrow the resource gaps in smaller companies that are more likely to be targeted by APTs through the provision of common threat intelligence platforms and collaboration among cybersecurity communities. These policy measures would also help bolster the national capacity to withstand cyber threats and make them in line with internationally accepted cybersecurity principles and frameworks.

The other major takeaway is that collaboration will be crucial, and sharing information will be crucial, to combat APTs. Well-coordinated threat actors working on APT campaigns can attack multiple sectors simultaneously, and a series of disjointed cybersecurity measures can be ineffective. The framework helps to share intelligence with other intelligence sharing programs to share indicators of compromise (IOCs), attack

patterns and mitigations. This collaborative effort improves understanding of the situation and the collective defence capability against new and emerging cyber threats.

D. Limitations and Future Research

While the results are encouraging, there were a number of caveats. One potential limitation was the number of experts in the panel (n=35) which could limit the generalizability of results obtained from the expert validation. The expert agreement scores are high, but there is a greater number of experts available for larger groups and more diverse groups can be recruited to provide more broad-based input on the applicability of and effectiveness of the cybersecurity frameworks. One other feature is the fact that a large number of the metrics reported are simulation based instead of based upon live deployments in organizations. While simulation environments can be useful to test and evaluate performance, they can also introduce other complexities like organizational resistance, infrastructure diversity and the intermittent character of attacks. The framework should thus be tested, validated in operational environments and in actual APT scenarios in future research. Empirical studies could be conducted in situations where MTTD, dwell time and efficiency of incidents could be accurately measured in the real world in organisations. Also, statistical evaluation of the significance and reliability of the performance improvement should be carried out by sector.

The framework requires more research to be expanded to new type of TTPs based on AI-enhanced cyber-attacks, automated attack campaigns, and adversarial machine learning techniques. It's important to keep the cyber threat landscape changing and adapting rapidly, and it's equally important to have a framework that can adjust to new technologies such as advanced analytics and AI. The framework could be replicated in other industries, geographic areas and organization-levels to make it more credible and relevant to high impact cybersecurity research. Such comparative analyses with other defense models could also be informative to study the best practices for APT mitigation. In short, this study shows that a full, all-around cyber security plan works well. This plan uses rules to enable Zero Trust, adheres to the MITRE ATT&CK model and looks at user behaviour to detect threats.

REFERENCES

[1] IBM, “What are advanced persistent threats (APTs)?,” IBM Security, 2024. [Online]. Available: https://www.ibm.com/think/topics/advanced-persistent-threats

[2] Vectra.ai, “Advanced persistent threat (APT) detection and defense guide,” Vectra AI, 2026. [Online]. Available: https://www.vectra.ai/topics/advanced-persistent-threat

[3] NIST, “NIST Cybersecurity Framework (CSF),” National Institute of Standards and Technology, 2022. [Online]. Available: https://www.nist.gov/cyberframework

[4] Premier Science, “Advanced persistent threats (APTs): Analysing tactics, techniques and impact,” *Premier Science Journal*, 2025.

[5] ISACA, “Cybersecurity insights: Emerging risks and resilience in organizations,” ISACA, 2021. [Online]. Available: https://www.isaca.org/resources

[6] Stimson Center, “Cybersecurity capacity in South Asia,” Stimson Center, 2025. [Online]. Available: https://www.stimson.org

[7] ISSRA, “Cyber threats to Pakistan’s critical infrastructure,” Institute for Strategic Studies, Research & Analysis (ISSRA), n.d.

[8] MITRE, “MITRE ATT&CK framework,” MITRE Corporation, 2024. [Online]. Available: https://attack.mitre.org

[9] ENISA, “Threat landscape for advanced persistent threats,” European Union Agency for Cybersecurity, 2023. [Online]. Available: https://www.enisa.europa.eu

[10] CyberSecurity Malaysia, “Cybersecurity insights: APTs and resilience in emerging economies,” CyberSecurity Malaysia, 2024. [Online]. Available: https://www.csm.my

[11] arXiv based SLR, “A systematic literature review on advanced persistent threat behaviors and detection strategies,” arXiv e-Print, 2025. [Online]. Available: https://arxiv.org/html/2503.11659v2

[12] ScienceDirect SLR, "A systematic literature review for APT detection and effective cybersecurity controls," Elsevier, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405844023043645
[13] NIST, "Zero Trust Architecture (NIST Special Publication 800-207)," National Institute of Standards and Technology, 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
[14] Zero Trust and Advanced Persistent Threats, "Zero Trust and advanced persistent threats: Who will win the war?," Franklin University, 2023. [Online]. Available: https://fuse.franklin.edu/context/facstaff-pub/article/1105/viewcontent/Zero_Trust_and_Advanced_Persistent_Threats.pdf
[15] arXiv based ZTA review, "Zero trust architecture: A systematic review," arXiv, 2025.
[16] ScienceDirect, "Design-oriented research in cybersecurity," *ScienceDirect*, 2013.
[17] Frontiers in Education, "Mixed methods research in cybersecurity education," *Frontiers in Education*, 2026.
[18] Cybersecurity Research Framework, "A framework for cybersecurity research," 2025.
[19] Mixed Methods IS, security studies, "Mixed methods in information security research," 2019.
[20] NCSC, "Threat report," National Cyber Security Centre, 2025.
[21] WJARR, "Cybersecurity frameworks for SMEs," *World Journal of Advanced Research and Reviews*, 2025.