

KENNETT_1908067

by Donna Kennett

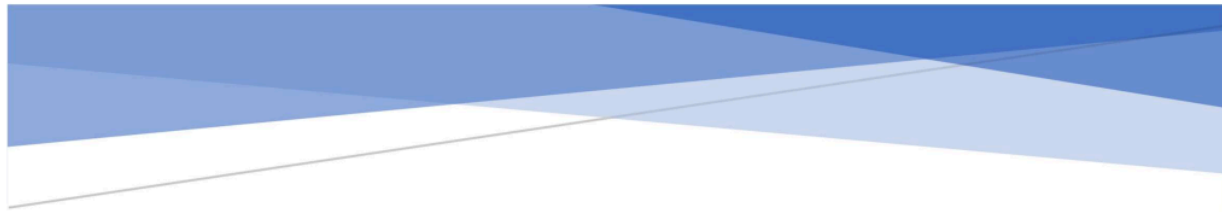
Submission date: 08-May-2026 02:02PM (UTC+0100)

Submission ID: 282801091

File name: 17418_Donna_Kennett_KENNETT_1908067_726821_610294377.docx (304.75K)

Word count: 5683

Character count: 39599



Emergent APT-Style Threat Actors: A Behavioural Comparison with Traditional APTs and Implications for Detection and Threat Hunting

ACCA7004 Research Methods and Professional Development Research Proposal

1908067 - Donna Kennett
1908067@student.uwtsd.ac.uk

Abstract

Advanced Persistent Threats (APTs) are traditionally described as technically sophisticated adversaries that conduct persistent, multi-stage intrusion campaigns. Recent cyber threat intelligence and incident-response reporting, however, highlights the emergence of APT-style groups that achieve similar impact through alternative tradecraft, particularly identity-centric and socially engineered intrusion techniques. This proposed study examines whether such emergent APT-style behaviours require different detection strategies from those developed for traditional APT models.

The study will adopt a mixed-methods comparative design, combining a PRISMA-informed systematic review with behavioural analysis using the MITRE ATT&CK framework and a conceptual experimental evaluation. Two behavioural datasets will be constructed: one representing traditional APT behaviours derived from academic literature, and one representing emergent APT-style behaviours informed by CTI, OSINT, and government sources. Comparative analysis will identify behavioural convergence and divergence, followed by an evaluation of detection performance using signature-based, behaviour-based, and identity-centric detection strategies.

The findings are expected to clarify whether existing detection approaches remain effective in contemporary threat environments and to inform practitioner-focused recommendations for detection engineering and threat-hunting strategies.

Keywords— APT detection, behavioural-centric, cyber threat intelligence, identity-centric intrusions, MFA fatigue, MITRE ATT&CK, open source intelligence, SIM swapping, sociotechnical, threat hunting

Table of Contents

Abstract.....	1
List of Tables	4
List of Figures	5
1. Introduction	6
1.1 Context and background.....	6
1.2 Research Problem	6
1.3 Research Aim and Objectives.....	7
1.3.1 Research Question	7
1.3.2 Aim	7
1.3.3 Objectives.....	7
1.4 Significance of the Research	7
1.4.1 Potential applications	7
2 Literature Review	8
2.1 Introduction	8
2.2 Key Contributions.....	8
2.2.1 Foundational APT behaviour and lifecycle modelling.....	8
2.2.2 Comparative Framework Analysis	8
2.2.3 Behavioural Detection and Analysis	10
2.2.4 Identity-Centric Intrusions and Modern Attack Vectors.....	10
2.2.5 CTI Evidence of APT-Like Behaviours in Emergent Groups.....	10
2.3 Gaps in the Literature	10
2.3.1 Limited Academic Coverage of Emergent APT-Style Groups	10
2.3.2 Insufficient Integration of Identity-Centric Behaviours into APT Models.....	10
2.3.3 Lack of Comparative Behavioural Studies.....	10
2.3.4 Dataset Limitations	10
2.5 Literature Summary	11
3 Research Design and Methodology	11
3.1 Introduction	11
3.2 Research Design	11
3.2.1 Methodology Framework (Saunders' Research Onion).....	12
3.3 Research Methods	12
3.3.1 Systematic Evidence Collection (PRISMA)	12
3.3.2 Comparative Behavioural Analysis.....	12
3.3.3 Conceptual Experimental Evaluation.....	13
3.4 Materials	13

3.5	Data Collection	14
3.6	Triangulation	14
3.7	Ethical Considerations.....	14
3.8	Limitations.....	14
4	Data Analysis.....	15
4.1	Comparative Behavioural Analysis.....	15
4.2	Conceptual Experimental Analysis.....	15
4.2.1	Variables and Hypotheses.....	15
4.2.2	Analytical Procedure	16
4.2.3	Detection Performance Metrics.....	16
5	Expected outcomes.....	16
4	Timeline.....	17
7	References	18
	Appendix A – PRISMA Evidence Extraction.....	21

List of Tables

Table 1: Identified Frameworks..... 9

Table 2: Research Design Overview 11

Table 3: Detection Strategies 13

Table 4: PRISMA stages 14

Table 5: Variables and Hypotheses 15

Table 6: Detection Performance Metrics and Measurement Approach 16

Table 7: Extracted Evidence Summary 21

List of Figures

Figure 1: Project timeline 17

Figure 2: PRISMA flow diagram 23

1. Introduction

1.1 Context and background

The cyber threat landscape is evolving. Alongside well-documented, state-sponsored Advanced Persistent Threats (APTs), a growing set of emergent actors has appeared that combines opportunistic behaviour with identity-centric and sociotechnical intrusion techniques. Despite limited technical sophistication, these actors have been linked to high-impact compromises that bypass conventional malware-focused detection and challenge established incident-response assumptions.

Cyber Threat Intelligence (CTI) provides the analytical foundation for understanding such adversaries, supporting detection, attribution, and defensive decision-making. Traditional APT activity has been characterised by persistent, strategic, and multi-stage intrusion campaigns aligned with long-term objectives. In response, CTI has increasingly shifted from reliance on isolated technical indicators toward behavioural analysis using structured frameworks such as MITRE ATT&CK®, recognising that adversary effectiveness lies in how actions are sequenced and adapted across the intrusion lifecycle rather than in individual tools or exploits.

Recent developments challenge these traditional assumptions. Identity-centric intrusions, such as credential theft, MFA fatigue, and abuse of cloud identity infrastructure, have become prevalent across modern attack campaigns, reflecting a strategic emphasis on access reliability and operational efficiency.

Industry reporting identifies identity compromise as a dominant intrusion vector, with Mandiant reporting stolen credentials in 16% of initial access cases and Microsoft analysing tens of millions of identity-risk detections daily, highlighting the scale and prevalence of identity-centric attack paths [1], [2].

Simultaneously, youth-driven and financially motivated APT-style groups have demonstrated the ability to compromise major organisations using accessible, socially engineered techniques rather than bespoke malware. These trends blur the boundary between cybercrime and state-aligned intrusion activity and expose limitations in existing APT behavioural models.

The growing importance of open-source intelligence (OSINT) further highlights this shift. OSINT provides timely visibility into emerging actors and techniques that are often absent from peer-reviewed literature, widening the gap between academic APT models and contemporary threat activity.

1.2 Research Problem

Although APTs are extensively examined in academic literature, existing research remains predominantly focused on state-aligned actors characterised by high technical sophistication and established intrusion patterns. In contrast, emergent APT-style groups, such as Lapsus\$ and Scattered Spider, exhibit identity-centric, socially engineered, and low-barrier intrusion behaviours that depart from these assumptions and are documented primarily through CTI, OSINT, and government reporting.

As a result, there is no integrated behavioural framework that systematically compares traditional APTs and emergent APT-style actors or assesses how their behaviours converge or diverge when mapped to a common structure such as MITRE ATT&CK®. This fragmentation, driven by both uneven evidence sources and academic models that emphasise bespoke tooling and long-term operational sophistication, creates uncertainty over whether detection strategies derived from traditional APT assumptions remain effective against contemporary, identity-centric intrusion behaviours.

1.3 Research Aim and Objectives

1.3.1 Research Question

Do emergent APT-style intrusion behaviours require different detection strategies from those traditionally used to detect traditional APT groups?

1.3.2 Aim

To determine whether emergent APT-style intrusion behaviours require different detection strategies from those used for traditional APT groups, through comparative analysis of two MITRE ATT&CK®-mapped behavioural datasets and a conceptual evaluation of detection performance.

1.3.3 Objectives

1. To systematically identify and extract behavioural evidence from academic, CTI, OSINT, and government sources.
2. To develop two MITRE ATT&CK®-mapped behavioural datasets representing traditional APT behaviours and emergent APT-style behaviours.
3. To identify behavioural convergence and divergence through thematic and comparative analysis.
4. To evaluate how different detection strategies perform when applied to both datasets.
5. To derive practitioner-relevant insights and recommendations for detection engineering and threat-hunting strategies based on observed detection performance differences.

1.4 Significance of the Research

This study addresses a growing misalignment between traditional academic APT models and contemporary intrusion behaviour. While established detection strategies are largely grounded in exploit-centric assumptions, modern attacks increasingly rely on identity compromise and sociotechnical methods. By constructing and comparing two structured behavioural datasets and evaluating detection performance across them, this research aims to provide a systematic, evidence-based assessment of whether emergent APT-style actors require alternative detection logic.

1.4.1 Potential applications

The findings are expected to inform detection engineering, threat-hunting workflows, and incident-response planning by clarifying how identity-centric intrusions differ from

conventional APT techniques. The research may also support improved threat modelling and risk assessment, contribute to academic understanding of hybrid and emergent threat actors, and inform CTI training and analyst education.

2 Literature Review

2.1 Introduction

Advanced Persistent Threats (APTs) have traditionally been characterised by strategic objectives, multi-stage intrusion chains, and long-term persistence within targeted environments [3], [4], [5]. Foundational research conceptualised APTs as adversaries capable of executing coordinated campaigns using structured attack sequences over extended periods [6], [7], [8]. These characteristics shaped early behavioural models and detection strategies, which focused on exploit-driven intrusion pathways and technical sophistication.

More recent CTI reporting highlights a shift in intrusion tradecraft, with identity compromise increasingly serving as a primary access vector for both state and non-state actors [1], [9], [10]. Academic work confirms that credential theft, MFA bypass, token hijacking, and cloud identity abuse are now common techniques, while behavioural detection research emphasises identity-driven anomaly identification [11], [12]. Industry reporting from Microsoft and Mandiant reinforces this trend, identifying identity compromise as a leading cause of modern breaches [1], [13]. As Evans notes, “attackers don’t hack in; they log in” [14], reflecting a broader transition away from exploit-centric attack paths.

2.2 Key Contributions

2.2.1 Foundational APT behaviour and lifecycle modelling.

The Cyber Kill Chain remains a foundational model for understanding APT operations, describing a sequential model of reconnaissance, exploitation, persistence and lateral movement [4], [15]. Subsequent academic work has expanded this model to define multi-stage intrusion patterns as a defining behaviour of APT campaigns [3], [16]. Together, these studies establish that APTs operate through predictable behavioural phases that can be modelled and analysed [4], [17], [18].

2.2.2 Comparative Framework Analysis

A substantial body of literature examines how analytical frameworks represent APT behaviour [19], [20]. Comparative analyses of the Cyber Kill Chain®, MITRE ATT&CK®, and the Diamond Model consistently conclude that MITRE ATT&CK® provides the most granular, technique-level representation of adversary behaviour, while the Diamond Model is better suited to adversary-centric and attribution-focused analysis [21], [22], [23], [24]. In response to the limitations of single-framework approaches, researchers have proposed unified cyber threat intelligence models that integrate lifecycle, behavioural, and adversary perspectives to improve analytical completeness [18].

Collectively, the literature demonstrates that no single framework fully captures the behavioural complexity of modern intrusion campaigns. Instead, researchers combine lifecycle-oriented models, behavioural taxonomies, identity-centric frameworks, and

CTI-driven mappings to analyse both traditional APT operations and emerging identity-driven threats. Table 1 summarises the key theoretical and technical frameworks identified in the literature, highlighting their focus, strengths, and limitations. For full details please see Appendix A (Table 7).

Table 1: Identified Frameworks

Framework/Model	Purpose/Focus	How it is used in the literature	Strengths	Limitations
Cyber Kill Chain® [4], [6], [15]	Linear intrusion lifecycle model describing sequential attack phases	Used to describe traditional APT operations, emphasising multi-stage behaviour	Clean structure; strong for modelling exploit-driven intrusions	Less effective for identity-centric or cloud-based attacks. Assumes linearity
MITRE ATT&CK® [17], [23], [25]	Behavioural-centric taxonomy of tactics and techniques	Used to map APT and identity-centric behaviours, comparative analysis across actors	High behavioural granularity; widely adopted in academic and CTI	Can be overwhelming. Uneven coverage across techniques
Diamond Model [21]	Adversary-centric model	Used for attribution-orientated analysis and understanding adversary intent	Strong for attribution and campaign-level analysis	Less detailed for technical behaviours. Limited identity-centric coverage
Unified CTI Models [18], [26]	Integrated frameworks combining Cyber Kill Chain, ATT&CK and Diamond Model	Used to improve analytical completeness and reduce model bias	Holistic; captures multiple dimensions of APT behaviour	Complex with limited adoption
Behavioural Analytics frameworks [15], [27], [28]	Detection models based on behavioural anomalies and long-term patterns	Used to detect stealthy APT behaviours, lateral movement, and privilege escalation	Effective for detecting unknown threats; adaptable	Requires high-quality telemetry. Prone to false positives
Identity-based attack taxonomies [11], [12], [14]	Classification of identity-centric attack vectors	Used to explain the shift from exploit-driven to identity-driven intrusions	Highly relevant to modern threat landscape	Still emerging. Limited academic standardisation
SSO/IAM security models [29], [30]	Frameworks analysing authentication flows and identity provider weaknesses	Used to examine SSO vulnerabilities and identity provider compromise	Strong for analysing authentication-layer attacks	Limited behavioural mapping
Cloud IAM Models (Azure AD, AWS IAM, GCP IAM) [1], [31]	Models describing cloud identity structures, permissions and attack paths	Used to analyse cloud identity compromise and privilege escalation	Essential for cloud-based APT and identity attacks	Rapidly evolving. Uneven documentation
CTI-driven behavioural frameworks [1], [2], [32]	Real-world behavioural mapping aligned with MITRE ATT&CK®	Used to document identity-centric intrusions, credential abuse, and modern APT-like behaviours	Empirical, up-to-date, operationally grounded	Not peer-reviewed. May lack methodological transparency

The identification and selection of academic, CTI, OSINT, and government sources informing this review followed a PRISMA-informed screening process, as illustrated in Appendix A (Figure 2).

2.2.3 Behavioural Detection and Analysis

Behavioural analytics is a dominant theme in APT detection research, reflecting the limitations of signature-based approaches against stealthy and adaptive adversaries [15]. Studies indicate that behavioural anomaly detection is more effective at identifying low-noise APT activity that evades traditional signatures, particularly when attacks are distributed over time [15]. Hybrid machine-learning approaches further improve detection by enhancing visibility into internal intrusion phases such as lateral movement and privilege escalation [28]. Systematic reviews confirm that long-term behavioural baselining is essential for detecting sophisticated and persistent intrusion campaigns [4], [15], [27], [33].

2.2.4 Identity-Centric Intrusions and Modern Attack Vectors

Research describes identity-based attacks as structured and repeatable techniques, including credential theft, MFA bypass, and access-token misuse [13], [34]. Analysis of authentication infrastructure highlight systemic weaknesses in Single Sign-On (SSO) mechanisms that enable authentication bypass [29] [32]. Complementary studies show how credential theft facilitates unauthorised access and persistence, while cloud-focused research demonstrates that compromise of identity and access management services in platforms such as Azure Active Directory, AWS IAM, and Google Cloud IAM enables control-plane access without reliance on traditional exploits [31].

2.2.5 CTI Evidence of APT-Like Behaviours in Emergent Groups

CTI reporting provides evidence of emergent actors exhibiting APT-like tradecraft. Microsoft's Digital Defence Reports identify identity compromise, cloud misconfiguration, and MFA fatigue as dominant intrusion vectors [1], [1], [35], [36]. Mandiant documents incidents in which attackers combine low-barrier identity attacks with advanced persistence techniques [2], [37], [38]. CrowdStrike provides OSINT-driven analysis of emergent groups adopting APT-style behaviours [32], while eSentire reports substantial growth in identity-driven intrusions and privileged-identity abuse [13].

2.3 Gaps in the Literature

2.3.1 Limited Academic Coverage of Emergent APT-Style Groups

Academic research continues to focus primarily on state-aligned APTs. Behavioural evidence relating to emergent APT-style groups remains largely confined to CTI and OSINT reporting rather than peer-reviewed literature.

2.3.2 Insufficient Integration of Identity-Centric Behaviours into APT Models

Traditional models such as the Cyber Kill Chain® do not adequately capture identity-driven intrusions, socially engineered access or cloud identity compromise.

2.3.3 Lack of Comparative Behavioural Studies

Despite CTI evidence of behavioural convergence, no academic studies systematically compare traditional APTs with emergent identity-centric actors.

2.3.4 Dataset Limitations

The evaluation of APT detection techniques is constrained by the scarcity of high-quality, publicly available datasets. Existing datasets are often narrowly scoped, synthetic, or

derived from partial observations, limiting their suitability for comprehensive behavioural analysis and empirical validation [39], [40].

2.5 Literature Summary

The literature demonstrates a clear evolution in intrusion behaviour. While traditional APTs remain defined by multi-stage, persistent operations captured by established frameworks such as the Cyber Kill Chain®, MITRE ATT&CK®, and the Diamond Model, identity-centric intrusions have become central to modern attack campaigns. CTI reporting shows that emergent, youth-based and financially motivated groups increasingly exhibit APT-like behaviours despite lower technical sophistication. These findings establish a strong foundation for comparative behavioural analysis while highlighting the absence of existing academic comparisons, reinforcing the originality and relevance of this research.

3 Research Design and Methodology

3.1 Introduction

This section outlines the proposed research design and methodological approach that will be used to examine whether emergent APT-style intrusion behaviours require different detection strategies from those applied to traditional APT groups. It describes the planned research design, methodological framework, data sources, analytical approach, and ethical considerations.

3.2 Research Design

This project will adopt a mixed-methods comparative design, integrating systematic evidence collection with a conceptual experimental evaluation. This design is appropriate because the research question concerns both behavioural differences between actor types and the practical implications for detection.

Table 2: Research Design Overview

Component	Description	Justification
Overall design	Mixed-methods comparative study combining systematic review, behavioural comparison, and conceptual evaluation	Supports structured behavioural analysis and detection assessment
Comparative element	Traditional APT behaviours vs emergent APT-style behaviours	Directly addresses behavioural divergence
Evaluation element	Detection-strategy assessment across two behavioural datasets	Enables evidence-based comparison
Evidence sources	Academic literature, CTI, OSINT, government advisories	Ensures triangulation and reduces source bias

Analytical framework	MITRE ATT&CK® mapping and thematic analysis	Provides a consistent, industry-aligned structure
Intended outcome	Determine whether emergent behaviours require different detection strategies	Aligns with the research aim

3.2.1 Methodology Framework (Saunders' Research Onion)

Methodological choices will be guided by Saunders' Research Onion to ensure consistency between philosophical assumptions, research strategy, and analytical methods.

The study will primarily adopt an interpretivist philosophy, as it seeks to analyse and compare intrusion behaviours, adversary tradecraft, and detection implications derived from academic and intelligence sources. Elements of post-positivism will be incorporated through structured comparison of behavioural datasets and evaluation of detection outcomes.

A deductive approach will be used, drawing on established APT theories to derive hypotheses concerning detection performance. The research will employ a mixed-methods strategy, combining qualitative behavioural analysis with comparative and evaluative techniques.

The research strategy will integrate:

- a PRISMA-informed systematic evidence review,
- comparative behavioural analysis using MITRE ATT&CK®, and
- a conceptual experimental evaluation of detection strategies.

A cross-sectional time horizon will be adopted, focusing on contemporary intrusion behaviours and current detection practices.

3.3 Research Methods

3.3.1 Systematic Evidence Collection (PRISMA)

A PRISMA-informed process will be used to identify and extract behavioural evidence from academic, CTI, OSINT, and government sources. Extracted data will include behavioural indicators, ATT&CK mappings, sociotechnical factors, detection implications, and source limitations.

3.3.2 Comparative Behavioural Analysis

Two categories of intrusion behaviour will be analysed:

- Traditional APT behaviours: exploit-driven, stealthy, lifecycle-based
- Emergent APT-style behaviours: identity-centric, socially engineered

Behaviours will be mapped to MITRE ATT&CK® techniques and analysed using thematic coding and cross-source triangulation to identify behavioural convergence and divergence relevant to detection.

3.3.3 Conceptual Experimental Evaluation

A conceptual experimental component will be used to evaluate whether detection strategies perform differently when applied to the two behavioural datasets. The evaluation of detection strategies in this study aligns with the Detect function of the NIST Cybersecurity Framework, providing a defensive context for assessing whether existing approaches remain effective against emergent APT-style behaviours [41], [42].

Three representative detection approaches will be assessed.

Table 3: Detection Strategies

Detection Strategy	Core Focus	Purpose in this research
Signature-based [4], [15], [43]	Known indicators and exploits	Baseline representing traditional APT detection
Behaviour-based [15], [27], [28], [44]	Anomalous system, network, or user behaviour	Evaluates generalisability across actor types
Identity-centric [11], [12], [29]	Authentication and identity misuse	Assesses effectiveness against emergent behaviours

Each detection strategy reflects a distinct set of assumptions about adversary behaviour identified in the literature, enabling comparative evaluation of how traditional and emergent APT-style behaviours interact with established detection patterns.

3.4 Materials

The study will make use of:

- Academic literature and systematic reviews,
- CTI reports from major vendors,
- Government advisories,
- OSINT investigations into emergent actors,
- PRISMA extraction tables,
- Constructed ATT&CK-mapped behavioural datasets, and
- Conceptual detection-logic templates.

No live malware, offensive tools, or operational systems will be used.

3.5 Data Collection

Data collection will follow the following four PRISMA stages to support consistency, transparency, and comparability across data sources.

Table 4: PRISMA stages

Stage	Method	Output	Justification
Identification	Searches across academic, CTI, OSINT, and government sources	Initial source pool	Ensures broad coverage of both traditional and emergent groups
Screening	Relevance filtering based on behavioural details and detection applicability	Reduced source set	Removes noise and ensures behavioural relevance
Eligibility	Exclusion of sources lacking behavioural evidence or methodological clarity	Final source list	Maintains quality and reliability of the dataset
Extraction	PRISMA table capturing behavioural evidence, ATT&CK mapping, social technical factors, biases	Structured dataset	Provides a consistent basis for comparison and experimentation

3.6 Triangulation

Triangulation will be used to enhance the validity and reliability of findings by integrating evidence from multiple independent sources. Given the fragmented nature of cybersecurity data, this approach will help mitigate bias and improve analytical robustness.

3.7 Ethical Considerations

The study will use only secondary data and simulated behavioural representations. No live systems, malware, or sensitive operational details will be involved. Behavioural modelling will be conducted exclusively through the MITRE ATT&CK® framework, and no personal or identifiable data will be processed. All sources will be cited responsibly.

3.8 Limitations

The study will rely on secondary reporting, which may reflect source-specific bias or incomplete visibility. Behavioural simulation cannot fully capture real-world attacker adaptability, and detection evaluation will be conceptual rather than operational. These limitations will be mitigated through structured analysis and evidence triangulation.

4 Data Analysis

This section outlines the analytical techniques that will be used to address the research objectives and evaluate the central research question. The analysis is divided into two stages: comparative behavioural analysis and conceptual experimental evaluation of detection performance.

4.1 Comparative Behavioural Analysis

Behavioural evidence extracted through the systematic review will be analysed using NVivo for thematic coding and MITRE ATT&CK-based clustering to compare traditional APT behaviours with emergent APT-style behaviours. Intrusion behaviours will be mapped to ATT&CK techniques to ensure consistent representation across both datasets.

The analysis will focus on identifying recurring behavioural patterns related to initial access, persistence, lateral movement, and reliance on identity compromise. Technique-level and tactic-level clustering will support structured comparison, while behavioural divergence will be identified by examining where emergent behaviours depart from assumptions embedded in traditional APT models.

4.2 Conceptual Experimental Analysis

Following the comparative analysis, a conceptual experimental evaluation will be undertaken to assess whether different detection strategies perform differently when applied to the two behavioural datasets.

4.2.1 Variables and Hypotheses

Table 5: Variables and Hypotheses

Category	Detail	Justification
Independent variable	Behavioural dataset type (traditional APT vs emergent APT-style)	Operationalises the core comparison
Dependent variables	Detection coverage, detection completeness, false-negative rate, detection consistency	Indicate detection effectiveness
Controlled variables	Detection strategies, dataset size, encoding method, evaluation criteria	Ensure fair comparison
Null hypothesis (H₀)	No difference in detection performance across datasets	Baseline expectation
Alternative hypothesis (H₁)	Detection strategies optimised for traditional APTs perform worse on emergent behaviours	Reflects expected behavioural divergence

These hypotheses directly test whether detection strategies derived from traditional APT assumptions remain effective when applied to emergent, identity-centric intrusion behaviours.

4.2.2 Analytical Procedure

The experimental evaluation will follow a structured analytical procedure:

1. Encode intrusion behaviours using MITRE ATT&CK® techniques.
2. Apply each detection strategy to both datasets.
3. Measure detection performance using predefined metrics.
4. Compare results across datasets to evaluate the stated hypotheses.

4.2.3 Detection Performance Metrics

Table 6: Detection Performance Metrics and Measurement Approach

Metric	Definition	Measurement Method	Relevance to Hypothesis Testing
Detection coverage	Proportion of behaviours identified by a detection strategy	Compare ATT&CK techniques present with those detected	Reduced coverage for emergent behaviours supports H ₁
Detection completeness	Extent to which intrusion stages are detected	Assess whether all, some, or none of the stages are identified	Fragmented detection indicates misalignment
False-negative rate	Proportion of behaviours not detected	Identify behaviours producing no detection output	Higher rates support H ₁
Detection consistency	Reliability of detection across similar behaviours	Evaluate detection as consistent or inconsistent	Inconsistency indicates strategy limitations

5 Expected outcomes

This research is expected to produce a primary analytical artefact in the form of two structured, MITRE ATT&CK-mapped behavioural datasets representing (i) traditional APT behaviours and (ii) emergent APT-style behaviours. The traditional APT dataset will capture multi-stage, persistent, and exploit-centric intrusion patterns derived from academic literature, while the emergent dataset will reflect identity-centric, socially engineered, and low-barrier behaviours documented in CTI, OSINT, and government reporting.

The artefact will support comparative analysis of traditional and emergent APT-style behaviours, identifying convergence and divergence across intrusion stages and enabling

evaluation of detection strategy effectiveness. The findings will be interpreted to provide practitioner-relevant insights into detection engineering and threat-hunting priorities, particularly in identity-centric attack scenarios.

4 Timeline

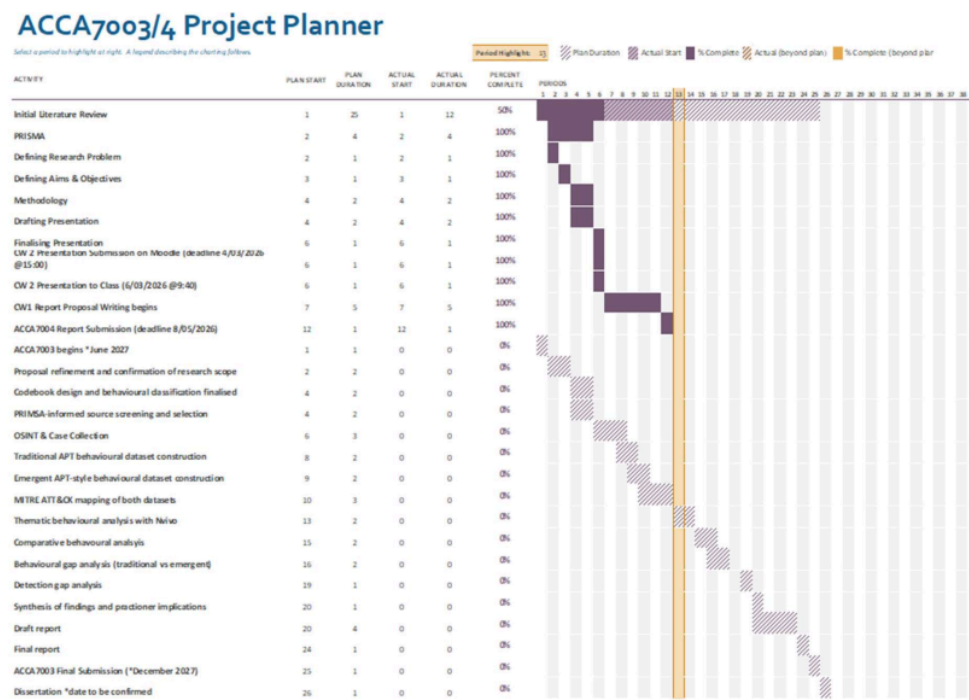


Figure 1: Project timeline

7 References

- [1] '2025 Microsoft Digital Defense Report (MDDR) | Security Insider'. Accessed: May 02, 2026. [Online]. Available: <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025>
- [2] 'M-Trends 2025: Data, Insights, and Recommendations From the Frontlines', Google Cloud Blog. Accessed: May 02, 2026. [Online]. Available: <https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025>
- [3] A. Khalid, A. Zainal, M. A. Maarof, and F. A. Ghaleb, 'Advanced Persistent Threat Detection: A Survey', in *2021 3rd International Cyber Resilience Conference (CRC)*, Jan. 2021, pp. 1–6. doi: 10.1109/CRC50527.2021.9392626.
- [4] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, 'A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities', *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019, doi: 10.1109/COMST.2019.2891891.
- [5] Y. Mei, W. Han, S. Li, and X. Wu, 'A Survey of Advanced Persistent Threats Attack and Defense', in *2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC)*, Oct. 2021, pp. 608–613. doi: 10.1109/DSC53577.2021.00096.
- [6] 'Cyber Kill Chain®', Lockheed Martin. Accessed: Feb. 28, 2026. [Online]. Available: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>
- [7] S. Yuldoshkhajev, M. Jeon, D. Kim, N. Nikiforakis, and H. Koo, 'A Decade-long Landscape of Advanced Persistent Threats: Longitudinal Analysis and Global Trends', in *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security*, Taipei Taiwan: ACM, Nov. 2025, pp. 3206–3220. doi: 10.1145/3719027.3765085.
- [8] Y. Xiuzhang *et al.*, 'A survey on intelligent detection for APT attacks', *China Communications*, vol. 22, no. 11, pp. 103–131, Nov. 2025, doi: 10.23919/JCC.fa.2023-0667.202511.
- [9] 'CISA and Partners Release Updated Advisory on Scattered Spider Group | CISA'. Accessed: Feb. 28, 2026. [Online]. Available: <https://www.cisa.gov/news-events/alerts/2025/07/29/cisa-and-partners-release-updated-advisory-scattered-spider-group>
- [10] 'Researchers Reveal Links Among LAPSUS\$, Scattered Spider, and ShinyHunters'. Accessed: Feb. 28, 2026. [Online]. Available: <https://cyberpress.org/lapsus-scattered-spider-shinyhunters-links/>
- [11] F. Al-Husari, O. Nakov, and P. Nakov, 'Multi-Factor Authentication Fatigue: A Growing Concern in User Experience and Security', in *2025 60th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)*, Jun. 2025, pp. 1–4. doi: 10.1109/ICEST66328.2025.11098219.
- [12] A. Pawale, B. Inchal, S. Bogur, Aditya, P. Redekar, and P. K. Sonwalkar, 'Beyond Passwords: The Essence and Impact of Multi-Factor Authentication in Cybersecurity', in *2025 6th International Conference for Emerging Technology (INCET)*, May 2025, pp. 1–5. doi: 10.1109/INCET64471.2025.11140909.
- [13] '2025 Identity Threat Research Report', eSentire. Accessed: May 02, 2026. [Online]. Available: <https://www.esentire.com/resources/library/identity-centric-threats-the-new-reality>
- [14] S. Sjouwerman, '[Eye Opener] Attackers Don't Hack, They Log In. Can You Stop Them?' Accessed: May 02, 2026. [Online]. Available: <https://blog.knowbe4.com/eye-opener-attackers-dont-hack-they-log-in.-can-you-stop-them>
- [15] A. Khalid, A. Zainal, M. A. Maarof, and F. A. Ghaleb, 'Advanced Persistent Threat Detection: A Survey', in *2021 3rd International Cyber Resilience Conference (CRC)*, Jan. 2021, pp. 1–6. doi: 10.1109/CRC50527.2021.9392626.
- [16] Z. Wang, Y. Zhou, H. Liu, J. Qiu, B. Fang, and Z. Tian, 'ThreatInsight: Innovating Early Threat Detection Through Threat-Intelligence-Driven Analysis and Attribution', *IEEE Transactions on Knowledge and Data Engineering*, vol. 36, no. 12, pp. 9388–9402, Dec. 2024, doi: 10.1109/TKDE.2024.3474792.

- [17] S. B. Son, S. Park, H. Lee, Y. Kim, D. Kim, and J. Kim, 'Introduction to MITRE ATT&CK: Concepts and Use Cases', in *2023 International Conference on Information Networking (ICOIN)*, Bangkok, Thailand: IEEE, Jan. 2023, pp. 158–161. doi: 10.1109/ICOIN56518.2023.10048930.
- [18] R. Odarchenko, A. Pinchuk, O. Polihenko, and A. Skurativskyi, 'A comparative analysis of cyber threat intelligence models'.
- [19] N. Naik, P. Jenkins, P. Grace, and J. Song, 'Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model', in *2022 IEEE International Symposium on Systems Engineering (ISSE)*, Oct. 2022, pp. 1–7. doi: 10.1109/ISSE54508.2022.10005490.
- [20] A. N. Irfan, S. Chuprat, M. N. Mahrin, and A. Ariffin, 'Taxonomy of Cyber Threat Intelligence Framework', in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, Oct. 2022, pp. 1295–1300. doi: 10.1109/ICTC55196.2022.9952616.
- [21] S.-S. Chen, T.-W. Pai, and C.-Y. Sun, 'Applying the Diamond Model of Intrusion Analysis with Generative Pre-trained Transformer 3', in *2023 International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan)*, Jul. 2023, pp. 289–290. doi: 10.1109/ICCE-Taiwan58799.2023.10226923.
- [22] T. Bierwirth, S. Pfützner, M. Schopp, and C. Steininger, 'Design and Evaluation of Advanced Persistent Threat Scenarios for Cyber Ranges', *IEEE Access*, vol. 12, pp. 72458–72472, 2024, doi: 10.1109/ACCESS.2024.3402744.
- [23] W.-T. Tsai, J.-N. Luo, and C.-L. Chou, 'Integrating Tree Structures with the MITRE ATT&CK Framework for APT Detection', in *2025 9th International Conference on Cryptography, Security and Privacy (CSP)*, Apr. 2025, pp. 139–143. doi: 10.1109/CSP66295.2025.00031.
- [24] M. S. Kulkarni, D. H. Ashit, and C. N. Chetan, 'A Proactive Approach to Advanced Cyber Threat Hunting', in *2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, Nov. 2023, pp. 1–6. doi: 10.1109/CSITSS60515.2023.10334219.
- [25] J. Uralov, S. Abdullaeva, I. Risolat, M. Yusupova, S. Kutliev, and M. Qazaqov, 'Using the MITRE ATT&CK Framework in SOC Activities and Analyzing Cyber Attack', in *2025 IEEE 26th International Conference of Young Professionals in Electron Devices and Materials (EDM)*, Jun. 2025, pp. 2160–2164. doi: 10.1109/EDM65517.2025.11096745.
- [26] N. Sun et al., 'Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives', *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1748–1774, 2023, doi: 10.1109/COMST.2023.3273282.
- [27] N. Saeed et al., 'Exploration of Behavior-Based Advanced Persistent Threat (APT) Detection: A Systematic Analysis based on Open CTI, MITRE ATT&CK, and Machine Learning', vol. 4, pp. 359–398, Mar. 2026.
- [28] M. Alrehaili, A. Alshamrani, and A. Eshmawi, 'A Hybrid Deep Learning Approach for Advanced Persistent Threat Attack Detection', in *Proceedings of the 5th International Conference on Future Networks and Distributed Systems*, in ICFNDS '21. New York, NY, USA: Association for Computing Machinery, Apr. 2022, pp. 78–86. doi: 10.1145/3508072.3508085.
- [29] T. Innocenti, L. Jannett, C. Mainka, V. Mladenov, and E. Kirda, '"Only as Strong as the Weakest Link": On the Security of Brokered Single Sign-On on the Web', in *2025 IEEE Symposium on Security and Privacy (SP)*, May 2025, pp. 1009–1027. doi: 10.1109/SP61157.2025.00024.
- [30] C. S. Johnson, M. L. Badger, D. A. Waltermire, J. Snyder, and C. Skorupka, 'Guide to Cyber Threat Information Sharing', National Institute of Standards and Technology, NIST SP 800-150, Oct. 2016. doi: 10.6028/NIST.SP.800-150.
- [31] K. Maidine and A. El-Yahyaoui, 'Cloud Identity Management Mechanisms and Issues', in *2023 IEEE 6th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech)*, Nov. 2023, pp. 1–9. doi: 10.1109/CloudTech58737.2023.10366178.

- [32] 'CrowdStrike Announces Release of 2024 Threat Hunting Report', CrowdStrike.com. Accessed: May 02, 2026. [Online]. Available: <https://www.crowdstrike.com/en-us/press-releases/2024-crowdstrike-threat-hunting-report-highlights-nation-states-exploits/>
- [33] Z.-S. Chen *et al.*, 'Clustering APT Groups Through Cyber Threat Intelligence by Weighted Similarity Measurement', *IEEE Access*, vol. 12, pp. 141851–141865, 2024, doi: 10.1109/ACCESS.2024.3469552.
- [34] 'Review of the Attacks Associated with LAPSUS\$ and Related Threat Groups'.
- [35] '2023 Microsoft Digital Defense Report (MDDR) | Security Insider'. Accessed: May 02, 2026. [Online]. Available: <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2023>
- [36] '2024 Microsoft Digital Defense Report (MDDR) | Security Insider'. Accessed: May 02, 2026. [Online]. Available: <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024>
- [37] 'M-Trends 2026: Data, Insights, and Strategies From the Frontlines', Google Cloud Blog. Accessed: May 02, 2026. [Online]. Available: <https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026>
- [38] 'M-Trends 2024: Our View from the Frontlines', Google Cloud Blog. Accessed: May 02, 2026. [Online]. Available: <https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2024>
- [39] S. Della Penna, R. Natella, V. Orbinato, L. Parracino, and L. Pianese, 'CTI-HAL: A Human-Annotated Dataset for Cyber Threat Intelligence Analysis', in *2025 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Jun. 2025, pp. 69–78. doi: 10.1109/EuroSPW67616.2025.00014.
- [40] A. A. Mamun, H. Al-Sahaf, I. Welch, M. Barcellos, and S. Camtepe, 'Limitations of Advanced Persistent Threat Datasets: Insights for Cybersecurity Research', in *2024 34th International Telecommunication Networks and Applications Conference (ITNAC)*, Nov. 2024, pp. 1–8. doi: 10.1109/ITNAC62915.2024.10815148.
- [41] J. L. Salas-Riega, Y. Riega-Virú, M. Ninaquispe-Soto, and J. M. Salas-Riega, 'Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats', *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 6, 2025.
- [42] National Institute of Standards and Technology, 'The NIST Cybersecurity Framework (CSF) 2.0', National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.
- [43] K. Xing, A. Li, R. Jiang, and Y. Jia, 'A Review of APT Attack Detection Methods and Defense Strategies', in *2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC)*, Jul. 2020, pp. 67–70. doi: 10.1109/DSC50466.2020.00018.
- [44] A. A. Mansur and T. Zaman, 'User Behavior Analytics in Advanced Persistent Threats: A Comprehensive Review of Detection and Mitigation Strategies', in *2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS)*, Nov. 2023, pp. 1–6. doi: 10.1109/ISAS60782.2023.10391553.

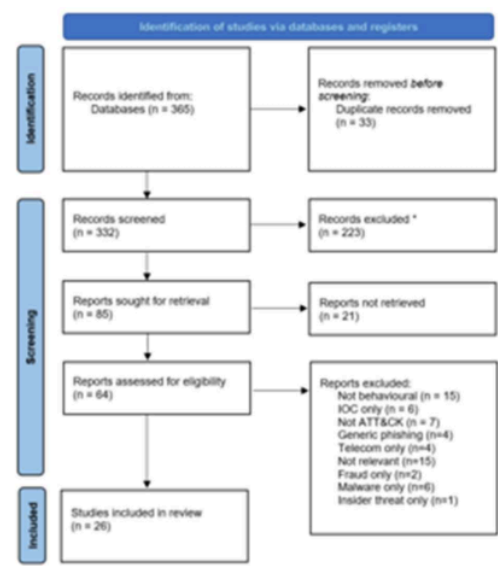
Appendix A – PRISMA Evidence Extraction

Table 7: Extracted Evidence Summary

Source ID	Source Type	Behavioural Evidence Identified	Framework(s) Referenced / Applicable
[1]	Industry CTI	Identity compromise, MFA fatigue, cloud identity abuse	MITRE ATT&CK® (Enterprise & Cloud)
[2]	Industry CTI	Credential-based initial access, persistence without exploits	CTI-driven behavioural frameworks
[3]	Academic survey	Behaviour-based APT detection, persistence characteristics	Behavioural analytics frameworks
[4]	Academic survey	Canonical multi-stage APT behaviour and lifecycle	Cyber Kill Chain®
[5]	Academic survey	Lifecycle-centric APT attack and defence strategies	Cyber Kill Chain®
[6]	Industry framework	Sequential intrusion lifecycle model	Cyber Kill Chain®
[7]	Academic longitudinal study	Long-term APT persistence and global trends	Lifecycle-based models
[8]	Academic survey	Intelligent and behaviour-based APT detection	Behavioural analytics
[9]	Government advisory	Credential theft, MFA fatigue, social engineering	MITRE ATT&CK® (implicit)
[10]	Industry / OSINT	Identity abuse and APT-like criminal behaviours	CTI-driven frameworks
[11]	Academic	MFA fatigue attacks	Identity-based attack taxonomies
[12]	Academic	MFA vulnerabilities and exploitation	Identity-centric models
[13]	Industry CTI	Growth in identity-driven intrusions	Identity-centric frameworks
[14]	Industry analysis	Conceptual framing of identity-centric intrusions	Identity threat models
[15]	Academic survey	Behaviour-based APT detection and baselining	Behavioural analytics
[16]	Academic	CTI-driven early threat detection and attribution	MITRE ATT&CK®, CTI models
[17]	Academic	ATT&CK concepts and use cases	MITRE ATT&CK®
[18]	Academic	Comparative analysis of CTI models	Unified CTI models
[19]	Academic comparative study	Attack-model comparison (Kill Chain, ATT&CK, Diamond)	Cyber Kill Chain®, MITRE ATT&CK®, Diamond Model

[20]	Academic	Taxonomy of CTI frameworks	Unified CTI models
[21]	Academic	Adversary-centric attribution analysis	Diamond Model
[22]	Academic	Simulated multi-stage APT scenarios	Cyber Kill Chain®
[23]	Academic	ATT&CK-integrated APT detection	MITRE ATT&CK®
[24]	Academic	Proactive threat-hunting approaches	Behavioural analytics
[25]	Academic	Operational ATT&CK usage in SOCs	MITRE ATT&CK®
[26]	Academic survey	CTI mining and behavioural intelligence	CTI-driven frameworks
[27]	Academic systematic review	Behaviour-based APT detection and baselining	Behavioural analytics
[28]	Academic	ML-based APT detection	Behavioural analytics
[29]	Academic	SSO authentication weaknesses	SSO / IAM models
[30]	Government standard	CTI sharing and lifecycle guidance	CTI lifecycle frameworks
[31]	Academic	Cloud IAM vulnerabilities and privilege escalation	Cloud IAM models
[32]	Industry CTI	Threat hunting and APT-like behaviours	CTI-driven frameworks
[33]	Academic	Behaviour-based clustering of APT groups	CTI-driven behavioural models
[34]	Government report	Identity-centric attack tradecraft (LAPSUS\$)	Identity-based frameworks
[35]	Industry CTI	Identity compromise trends	Identity-centric frameworks
[36]	Industry CTI	Identity and cloud attack evolution	Identity-centric frameworks
[37]	Industry CTI	Credential-based initial access	CTI-driven frameworks
[38]	Industry CTI	Threat landscape evolution	CTI-driven frameworks
[39]	Academic	CTI dataset limitations	Methodological support
[40]	Academic	Limitations of APT datasets	Methodological justification
[41]	Academic review	NIST CSF implementation	Defensive context
[42]	Government framework	Cybersecurity risk management	NIST CSF
[43]	Academic review	APT detection and defence strategies	Detection baseline
[44]	Academic	User behaviour analytics for APTs	Behavioural analytics

PRISMA flow diagram illustrating the proposed study identification, screening, eligibility, and inclusion process.



*No automation tools were used.

Figure 2: PRISMA flow diagram

FINAL GRADE

GENERAL COMMENTS

87 /100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7



Comment 1

Support with the literature

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

PAGE 21

PAGE 22

PAGE 23

PAGE 24

GRADING FORM: ACFA7004 PROPOSAL MAY 2026

DONNA KENNETT

87

ENGAGEMENT WITH LIT.SKILL [30]

Structure and Organization of the literature review [8 Marks] Critical Engagement with Literature [10 Marks] Relevance and Positioning of Your Study [7 Marks] Recent and Relevant in-text citations and reference list [5 Marks]



The literature review is well structured and thematically organised,
There is good critical evaluation and synthesis of frameworks and approaches, although reliance on CTI/OSINT limits some academic depth and

27

methodological transparency.
The research gap is clearly identified
Sources are relevant and well integrated,

KNOWLEDGE & UNDERSTANDING [20]

Brief overview and current developments in the proposed research area [10 Marks] Research problem statement [7 Marks] Significance of the study [3 Marks]



The proposal demonstrates strong and current understanding of APT behaviours, identity-based threats, and CTI frameworks.

The research problem is clearly articulated and logically developed, but it needs to be supported by the literature.

The significance is clearly defined and well aligned with current real-world challenges

16

COGNITIVE & INTELLECTUAL [10]

Clearly state the aim of the research based on the identified research problem [5] Break down the research aim into smaller, measurable, and achievable steps [5]



The aim is clear, focused, and well aligned with the research problem.

The objectives are well structured,

9

PRACTICAL APPLICATION [25]

*Research Design (Explanation of the overall research approach) [7]
Research methods [10] - a detailed explanation about the research*

methods to achieve the research objectives Research materials [8] - in terms of Software and hardware

21



The research design is appropriate and well justified.

The methodology is clear and well structured, but the evaluation is mainly conceptual, which limits how strong and practical the results will be.

The materials are appropriate for the proposed design

TRANSFERABLE SKILLS [15]

Project planning and resource management [5 Marks] Description of the project's potential impact and limitations [5 Marks] - Expected outcome Presentation style [5 Marks]

14



The project timeline is clearly stated

Limitations are clearly identified and critically acknowledged

The writing is clear, coherent, and academically strong