

Presentation PDF

by Donna Kennett

Submission date: 01-Mar-2026 05:35PM (UTC+0000)

Submission ID: 276191754

File name: 17418_Donna_Kennett_Presentation_PDF_726817_1677057601.pdf (799.9K)

Word count: 1356

Character count: 9149



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

ACFA7004 Project Proposal

Donna Kennett

1908067@student.uwtwd.ac.uk

Project Background and Context

- Traditional Advanced Persistent Threat (APT) groups are well studied and follow structured, long-term intrusion patterns [1,2].
- New emergent APT-style groups (e.g. Scattered Spider, Lapsus\$ etc.) use faster, identity-centric and socially engineered attacks [3].
- Academic research heavily covers traditional APTs but offers little on newer actor types [1].
- This creates a gap in understanding how emerging groups behave and how to detect them effectively [1,3].

Professional Context

- ▶ Senior SOC Specialist for the UK government
- ▶ Lead threat hunting, Threat Intelligence, and Incident Management response

Practical Experience

- Manage real-world intrusion and malware analysis
- Conduct threat hunting in complex enterprise environment
- Behavioural analysis and detection engineering using MITRE ATT&CK®[4], Cyber Kill Chain®[5] and Diamond Model of Intrusion analysis [6].
- Hands on experience with identity-centric and emergent threat actor behaviours

Relevant Professional Certifications:



Research Problem

- Existing APT behavioural models no longer fully describe modern, identity-driven intrusion activity [1].
- Emergent groups use non-traditional, opportunistic and high-impact behaviours (e.g. SIM Swapping, MFA Fatigue etc.) [3,7,8].
- These behaviours are poorly represented in academic literature and ATT&CK-aligned defensive models [1,9].
- As a result, defenders face detection blind spots for these new threat types [1,3]

Research Aim

To analyse emergent APT-style actor behaviours, compare them with traditional APTs, and develop evidence-based detection and threat-hunting recommendations.

Research Questions

1. What behaviours define traditional APT groups?
2. What behaviours do emergent APT-style actors exhibit?
3. How do emergent behaviours differ from traditional APT behaviours?
4. What detection opportunities or gaps arise from these differences?

Research Objective

1. To conduct a structured literature review of behavioural patterns, tactics and techniques used by traditional APT groups compared with emergent APT groups.
2. To analyse emergent APT-style cases through OSINT (Open-Source Intelligence) to fill the intelligence gap revealed in the first literature review.
3. To map and **compare** behaviours using the industry recognised MITRE ATT&CK framework [4].
4. To produce detection-engineering and hunting recommendations for emergent APT-style groups

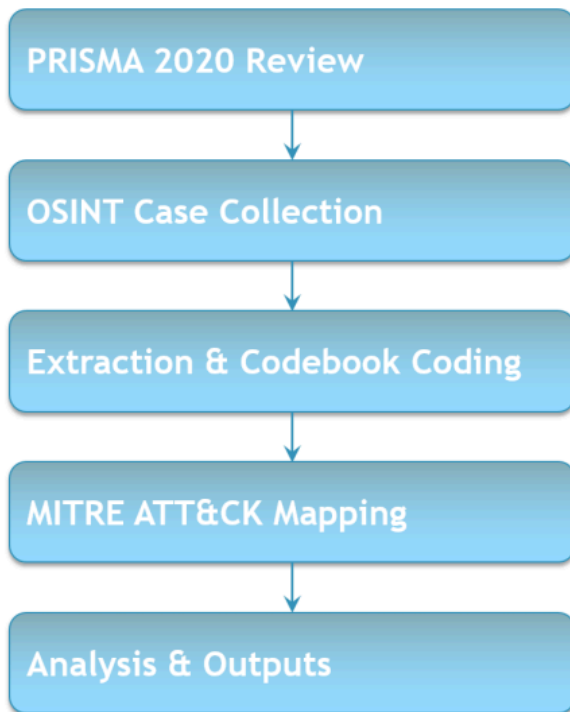
Research Design Alignment Table

Objective	Research Question	Methods	Output
1. Literature review of traditional APTs	1. What behaviours define traditional APT groups?	• PRISMA 2020 • Database search • ATT&CK mapping	Traditional APT behavioural baseline
2. Analyse emergent APT-style actors	2. What behaviours do emergent APT-style actors exhibit?	• OSINT • Codebook coding • Confidence scoring	Emergent actor TTP dataset & profiles
3. Map & compare traditional vs emergent groups	3. How do emergent behaviours differ from traditional APT behaviours?	• Thematic analysis • Comparative analysis	ATT&CK-mapped comparison & behavioural models
4. Produce detection & hunting recommendations	4. What detection opportunities or gaps arise from these differences?	• Detection-gap analysis • Synthesis	Detection logic & hunting hypotheses

Research Onion - Methodology Table

Layer	Method	Justification
Research Philosophy	Interpretivism (with Pragmatist elements)	Interpreting behaviours, motivations and patterns. Pragmatism supports combining academic and CTI sources
Research Approach	Inductive	Not testing a hypothesis; deriving behavioural patterns from the data.
Research Strategy	System Literature Review & Comparative Analysis	PRISMA 2020 ensures transparency and replicability. Comparative analysis allows structured comparison of traditional APTs vs emergent APT-style groups.
Methodological Choice	Qualitative & Thematic Analysis	All data is textual (papers, CTI reports). Behavioural coding using MITRE ATT&CK is qualitative and pattern-focused.
Time Horizon	Cross-Sectional	Analysing existing literature at a single point of time to identify gaps in academic coverage. Not tracking threat actor evolution.
Techniques & Procedures	PRISMA search, Screening, Data Extraction, ATT&CK Coding, Behavioural Comparison	PRISMA 2020 documents the search and screening process. ATT&CK provides a structured behavioural coding framework. Comparative analyst highlights behavioural differences.

Methodology Overview



Methodology Flow Diagram

Systematic Literature Review

PRISMA 2020 for structured evidence gathering [1]

Data Collection and Coding

OSINT cases coded with predefined codebook

Standardisation

MITRE ATT&CK for consistent behaviour mapping [4]

Analysis and Synthesis

Identify pattern with thematic and comparative analysis and build behavioural models

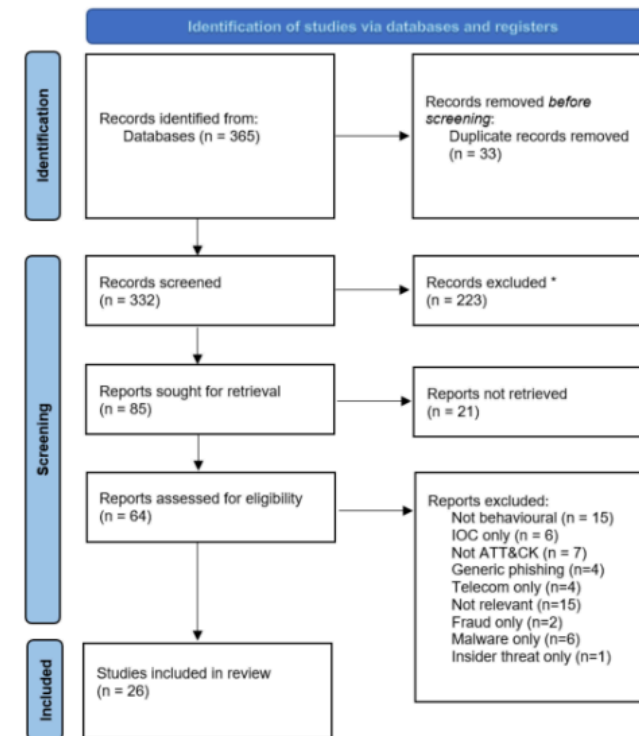
PRISMA 2020 Literature Review

Purpose

- Transparent and systematic search
- Reduces selection bias
- Identifies research gaps
- Supports replicability

Summary

- Identification (365 identified and 33 removed)
- Screening (332 screened with 223 excluded)
- Eligibility (64 assessed and 38 excluded)
- Included 26 studies



*No automation tools were used.

PRISMA Flow Diagram

Case Study Selection

- Two emergent APT-style groups will be selected from reliable OSINT sources [1].
- To be chosen due to public reporting, behavioural novelty and limited academic study.
- To enable examination of identity-centric and socially engineered intrusions.
- To create a strong contrast with structured, traditional APT groups

Data Extraction & Coding

- Pre-defined codebook will ensure consistent TTP (Tactic, Techniques and Procedures) classification.
- Metadata and confidence levels will be recorded for each observation.
- All TTPS will be mapped to ATT&CK standardised behaviours [4].
- This will ensure transparency, reproducibility, and consistency across cases.

Analytical Techniques

1. Thematic Analysis: to identify behavioural clusters [1].
2. Cross-Cluster Analysis: to understand relationships between behaviours.
3. Comparative Analysis: to contrast traditional vs emergent groups.
4. Detection-Gap Analysis: to identify weaknesses in current detection models.
5. Model Synthesis: to produce high-level behavioural representations.

Expected Outputs

- ✓ ATT&CK-mapped behavioural comparison
- ✓ High-level behavioural models
- ✓ Detection-engineering recommendations
- ✓ Threat-hunting hypotheses
- ✓ Replicable research methodology

Expected Impact

- ✓ Improved understanding of emergent intrusion behaviours
- ✓ Stronger detection coverage for identity-based attacks
- ✓ Updated behavioural models for analysts and defenders
- ✓ Provides a transparent repeatable approach for future research

Resources Required for the Project

Core Research Tools

- PRISMA 2020 tools - for structured transparent literature screening
- MITRE ATT&CK Navigator - for mapping and comparing TTPs
- Microsoft Excel - for coding matrices, data extraction and analysis

Academic & Writing Support

- Reference Manager (Zotero) - for citations and source organisation
- Note-taking tool (Obsidian) - for coding notes, audit trail and reflections

Technical & Practical Requirements

- Computer & reliable internet access
- Access to IEEE Xplore and ScienceDirect via University Library
- Standard O365 software (Word and PowerPoint) - for producing deliverables

Risk and Mitigation Strategies

Risk	Description	Likelihood	Impact	Mitigation Strategies
1. Data Gaps	Some actors lack detailed public reporting	Medium	High	• Use backup cases • Apply triangulation
2. Scope Creep	Project may expand beyond planned boundaries	Medium	Medium	• Follow aims & SMART objectives • Review scope weekly
3. Time Pressure	Limited weekly study time increased deadline risk	High	High	• Fixed study blocks • Buffer week
4. Source Inconsistencies	OSINT quality and detail vary significantly	High	Medium	• Predefined codebook and ATT&CK mapping • Confidence scoring
5. Analytical Ambiguity	Some behaviours are difficult to classify	Medium	Low	• Maintain audit trail • Justify coding choices

Project Timeline

ACCA7003/4 Project Planner

Select a period to highlight at right. A legend describing the charting follows.

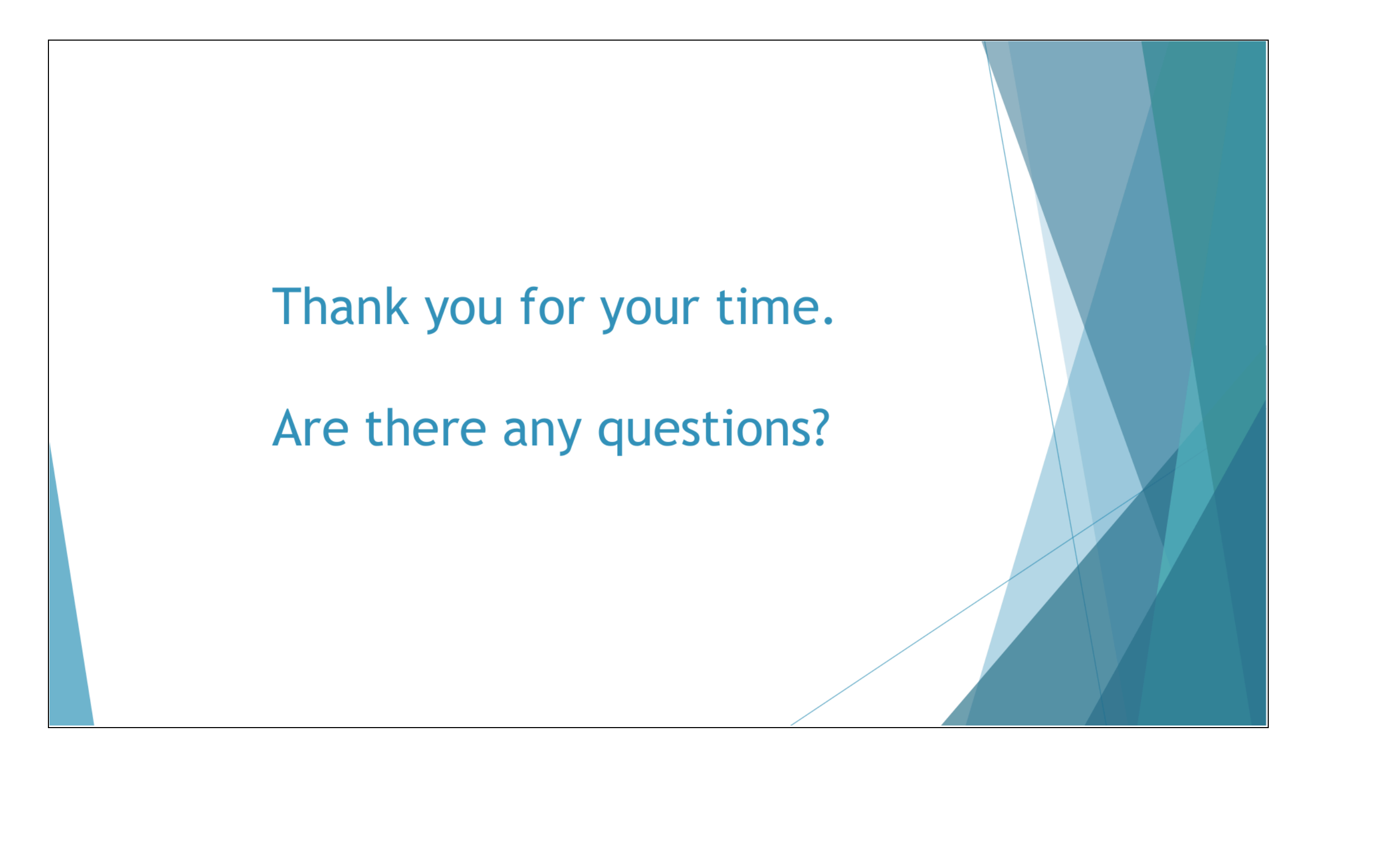


Conclusion

- Proposal delivers a structured plan to analyse emergent APT-style actors
- Combines PRIMSA, ATT&CK mapping, thematic analysis and comparative methods
- Produces actionable detection insights and updated behavioural models
- Contributes both academically and practically to cyber-defence research

References

- [1] N. I. Che Mat, N. Jamil, Y. Yusoff, and M. L. Mat Kiah, 'A systematic literature review on advanced persistent threat behaviors and its detection strategy', *J Cyber Secur*, vol. 10, no. 1, p. tyad023, Jan. 2024, doi: [10.1093/cybsec/tyad023](https://doi.org/10.1093/cybsec/tyad023).
- [2] C. Ekisa, D. Ó Briain, and Y. Kavanagh, 'Leveraging the MITRE ATT&CK Framework for Threat Identification and Evaluation in Industrial Control System Simulations', in *2024 35th Irish Signals and Systems Conference (ISSC)*, Jun. 2024, pp. 1–6. doi: [10.1109/ISSC61953.2024.10602968](https://doi.org/10.1109/ISSC61953.2024.10602968).
- [3] '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>
- [4] 'MITRE ATT&CK®'. Accessed: Feb. 28, 2026. [Online]. Available: <https://attack.mitre.org/>
- [5] 'Cyber Kill Chain®', Lockheed Martin. Accessed: Feb. 28, 2026. [Online]. Available: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>
- [6] 'The Diamond Model of Intrusion Analysis'. Accessed: Feb. 28, 2026. [Online]. Available: <https://apps.dtic.mil/sti/citations/ADA586960>
- [7] 'Researchers Reveal Links Among LAPSUS\$, Scattered Spider, and ShinyHunters'. Accessed: Feb. 28, 2026. [Online]. Available: <https://cyberpress.org/lapsus-scattered-spider-shinyhunters-links/>
- [8] 'Resecurity | Trinity of Chaos: The LAPSUS\$, ShinyHunters, and Scattered Spider Alliance Embarks on Global Cybercrime Spree'. Accessed: Feb. 28, 2026. [Online]. Available: <https://www.resecurity.com/blog/article/trinity-of-chaos-the-lapsus-shinyhunters-and-scattered-spider-alliance-embarks-on-global-cybercrime-spree>
- [9] N. H. A. Mutalib, A. Q. M. Sabri, A. W. A. Wahab, E. R. M. F. Abdullah, and N. AlDahoul, 'Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: a review', *Artif Intell Rev*, vol. 57, no. 11, p. 297, Sep. 2024, doi: [10.1007/s10462-024-10890-4](https://doi.org/10.1007/s10462-024-10890-4).



Thank you for your time.

Are there any questions?

Presentation PDF

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

82/100

Further to the comments provided during the presentation, please follow the feedback provided for each category in the rubric.

Also, an artefact needs to be developed as part of the project.

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

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

GRADING FORM: ACFA7004 PROPOSAL PRES 2026

DONNA KENNETT

82

ENGAGEMENT WITH LIT.SKILL [20]

Relevant and recent Literature support for Research background/context [7 Marks] Recent Literature support for the identified research problem [7 Marks] Recent and Relevant in-text citations and reference list [6 Marks]

 An adequate list of literature is provided. Also a detailed plan of SLR demonstrated. Research background is supported with literature and also clearly stated the Research problem. **18**

KNOWLEDGE _ UNDER.. SKILLS[15]

Brief overview and current developments in the proposed research area [10 Marks] Research problem statement [5 Marks]

 A brief overview of the current stage is well presented. Clear research problem with literature support **15**

COGNITIVE&INTELL. SKILLS[20]

Formulation of research aim and objective based on the identified research problem [20 Marks]

 Research aim, objectives and RQs are presented. The aim is in line with the research problem. However, the RQs and objectives needs to be aligned. And for research questions hypothesis needs to be considered. **15**

PRACTICAL APPN SKILLS[25]

Selection of appropriate research methods and materials to achieve the research objectives, with justification [15 Marks]
Details of the data collection and evaluation process [10 Marks]

 Proposed research methods are adequate for the selected problem. However these need to be justified with the literature. Also detailed explanation of the data and collection methods are expected.

19

TRANSF. SKILL & PROF.PRAC [20]

Project planning and resource management [10 Marks] Description of the project's potential impact and limitations [5 Marks] Presentation style [5 Marks]

 Revisit the project plan and update based on the timeline, Include limitations. it was a well presented presentation. Well done

15