

```
MmsaeDishcx IndtePsych ';&($Velorgan01) (Fangle  
Para$MultifHypnooboglur DrabuUnextd Sudas  
GuitaParaleChucktSpecit Tick2Jaund=Whole$ Koorel  
AurivSaltl:EllevwEnsobicafetnfejlsd RoquiSambar  
Velorgan01) (Fanglette9 '  
torde$SuedeBklorerErectedecayvCitraiDannegPhysi  
SystfBungmo overrcloniuGertid SmoksgraesaPrereel  
Obtetnitro2  
Unde+Decat$AdvenBYieldrColleeBeleavAfskriLagreg  
Velorgan01) (Fanglette9 'Rolan$DelagCFalcihUdal  
FunkpVandeelremenPatriiTolvm Ebbes=Ungdo Dekom(  
RezogAfskrwStegem UnuniTaffy NonvwPneumiSartkn  
Diop2Feltm_SpookpKontir Inclo Arvec Pusse Relas  
Eury-PreocFVorti UnfaiPStoltrSolskoGngetcSussiel  
seIFarefdUdsla=Lever$Krste{MangrP OmstIKonfeDIndik}  
Nedri.SoileCSaxdioIntermKappem EsliaRealvnBortf
```

Student ID number:	2316422
Programme:	MSC Cybersecurity and Digital Forensics
Module:	Research Methods and Professional Development
Module code:	ACFA7004
Assignment Title:	Presentation
Lecturer:	Dr Seena Joseph

Working Title:
Investigating and developing technical controls that are effective at preventing fileless malware infections

Research context and background

Malware	Fileless Malware
Can be detected with signature based detection	Can't be detected with signature based detection
Source code	No source code
Malicious processes	No malicious process (uses trusted processes)
Installs itself, alters file system, leaves traces on disk	Executes in memory, doesn't leave traces on disk

Fig 1. Malware and fileless malware comparison

Relevant and recent Literature support

Description of the problem with literature support

Research problem statement

Lack of research on the technical controls that could prevent fileless malware infections

Paper	Methodology	Mitigation with specific technical controls
[1] Sudhakar and S. Kumar, "An emerging threat Fileless malware: a survey and research challenges," <i>Cybersecur</i> , vol. 3, no. 1, -01-14 2020. doi: 10.1186/s42400-019-0043-x.	Survey paper, Discusses monitoring system behavior, rule-based detection and behavioural analysis of event logs	No
[2] I. Kara, "Fileless malware threats: Recent advances, analysis approach through memory forensics and research challenges," <i>Expert systems with applications</i> , vol. 214, pp.119133, Mar 15 2023. doi: 10.1016/j.eswa.2022.119133. Available: https://dx.doi.org/10.1016/j.eswa.2022.119133	Develops a memory analysis detection approach	No
[3] N. Singh and S. Tripathy, "Unveiling the veiled: An early stage detection of fileless malware," <i>Computers & security</i> , vol. 150, pp.104231, Mar 2025. doi: 10.1016/j.cose.2024.104231. Available: https://dx.doi.org/10.1016/j.cose.2024.104231	A software is developed that extracts key features of memory dumps in real time for fileless malware detection	No
[4] Vala Khushali, "A Review on Fileless Malware Analysis Techniques," <i>International journal of engineering research & technology (Ahmedabad)</i> , vol. 9, no. 5, May 9 2020. doi: 10.17577/IJERTV9IS050068. Available: https://www.ijert.org/research/a-review-on-fileless-malware-analysis-techniques-IJERTV9IS050068.pdf	This paper carries out a literature review in order to define existing malware and detection techniques	Briefly – One paragraph
[5] F. A. Demmese, et al., "Machine learning based fileless malware traffic classification using image visualization," <i>Cybersecurity</i> , vol. 6, no. 1, pp.32–18, Dec 1 2023. doi: 10.1186/s42400-023-00170-z. Available: https://link.springer.com/article/10.1186/s42400-023-00170-z	Using Machine learning and image visualisation to identify fileless malware network traffic	No
[6] O. Khalid, et al., "An Insight into the Machine-Learning-Based Fileless Malware Detection," <i>Sensors (Basel, Switzerland)</i> , vol. 23, no. 2, pp.612, Jan 5 2023. doi: 10.3390/s23020612. Available: https://www.ncbi.nlm.nih.gov/pubmed/36679406	Combines machine learning with memory analysis to identify fileless malware	No

Table 1. Summary of relevant academic literature

Recent Literature support for the identified research problem

upload malware and modify system settings without the file system.

Fileless Malware Detection is finding a new approach to the executable in the system. In the detection process also use traditional approaches like Sandboxing, execution emulation using tools such as ProcMon, Yara, and heuristics-based.

Fileless Malware useful some Mitigation points:

- Perform OS patches and updates periodically.
- Restrict the PowerShell usage policy to restricted access to run the scripts through windows policy.
- Perform Behavior-based analysis.
- Periodically check the recent patches for vulnerabilities in the application and security checks frequently.

PSDEM: A Fileless PowerShell Detection Method for Malicious PowerShell Detection [2]

tool takes different actions and gets original scripts once the regex designed according to the features of different obfuscation methods matches successfully.

1. Further Analysis

The tool has got original PowerShell scripts in Word documents. So, attack to easily understand now. The scripts are used downloader, visit malicious websites and saving payload in the folder called temp. The scripts .exe file has downloaded in the backstage. The tool will extract the payload and URLs to analyze.

III. LITERATURE REVIEW AT GLANCE

Sr. No.	Title of Paper	Major Contribution	Further extension
1	A Survey on Malware Analysis Techniques	Explain Malware types, Detection methods,	Memory Analysis gives detailed

[4] Vala Khushali, "A Review on Fileless Malware Analysis Techniques," *International journal of engineering research & technology* (Ahmedabad), vol. 9, no. 5, May 9 2020. doi: 10.17577/IJERTV9IS050068. Available: <https://www.ijert.org/research/a-review-on-fileless-malware-analysis-techniques-IJERTV9IS050068.pdf>

Research aim and objectives

Research Aim:	This research aims to investigate technical security controls that are effective at defending against fileless malware infections
Objective 1:	To carry out a thorough investigation into fileless malware's operation, existing analysis techniques and existing mitigations by reviewing academic literature.
Objective 2:	To collect fileless malware samples and analyse them in a safe environment using static analysis, dynamic analysis and memory analysis.
Objective 3:	Based on the findings, identify current technical controls and develop new technical controls that are effective in preventing fileless malware infections.
Objective 4:	Evaluate the effectiveness of the identified and developed controls against popular anti-virus solutions using an established measurement methodology

Table 2. Research aims and objectives

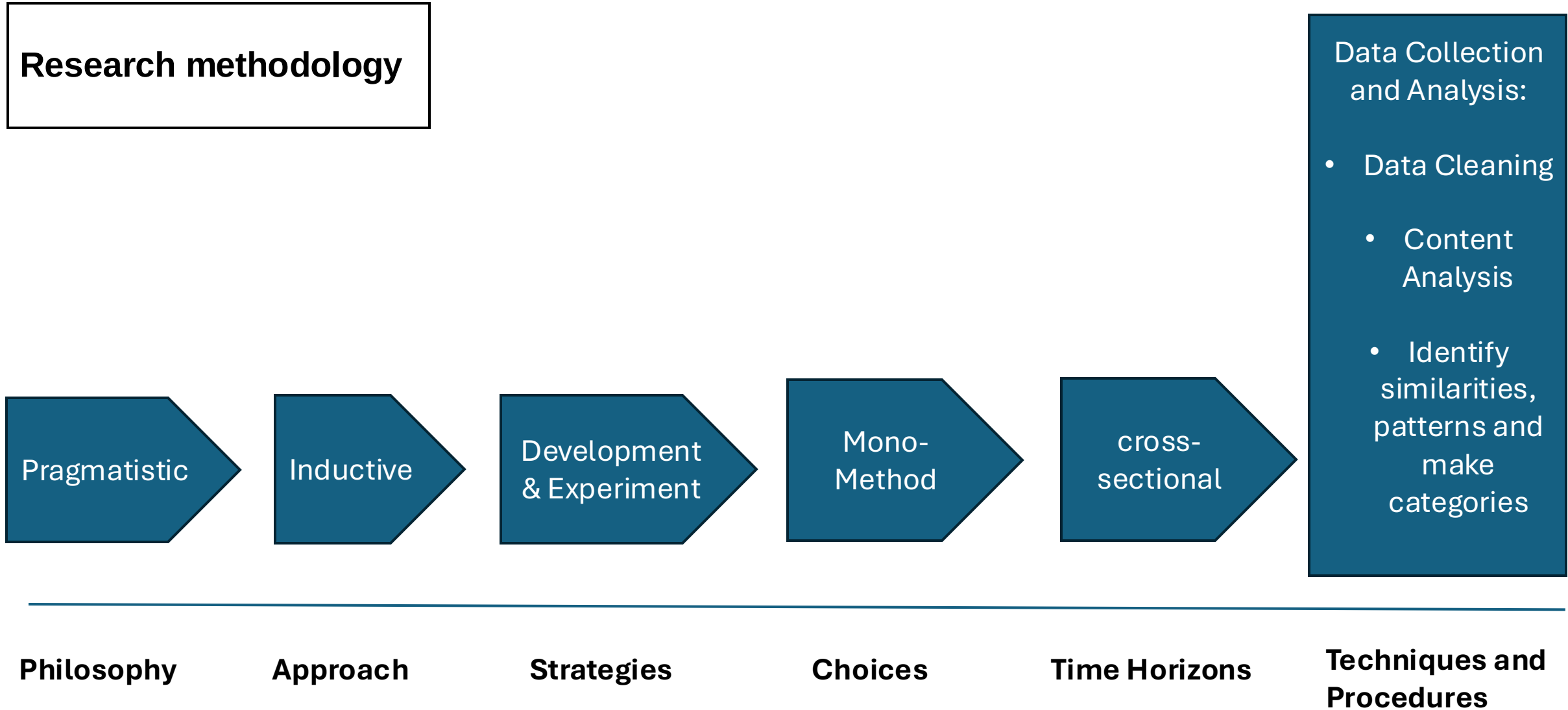


Fig 2. Research Methodology following the categories of the research onion

Research methodology

Preperation stage

Create analysis environment(s)



Locate sources of Malware



Download Malware samples

Malware Analysis Pipeline

Identifying the format of a malware sample (e.g. Binary or source code, windows / linux)



Static Analysis (Using disassembly if in binary format)
Program analysis, statistical analysis of the files contents



Dynamic Analysis using an analysis environment.



Memory Analysis on a workstation not connected to the internet

[8]

Identification and design of controls, testing and evaluation

Study results



Identify and develop controls based on results



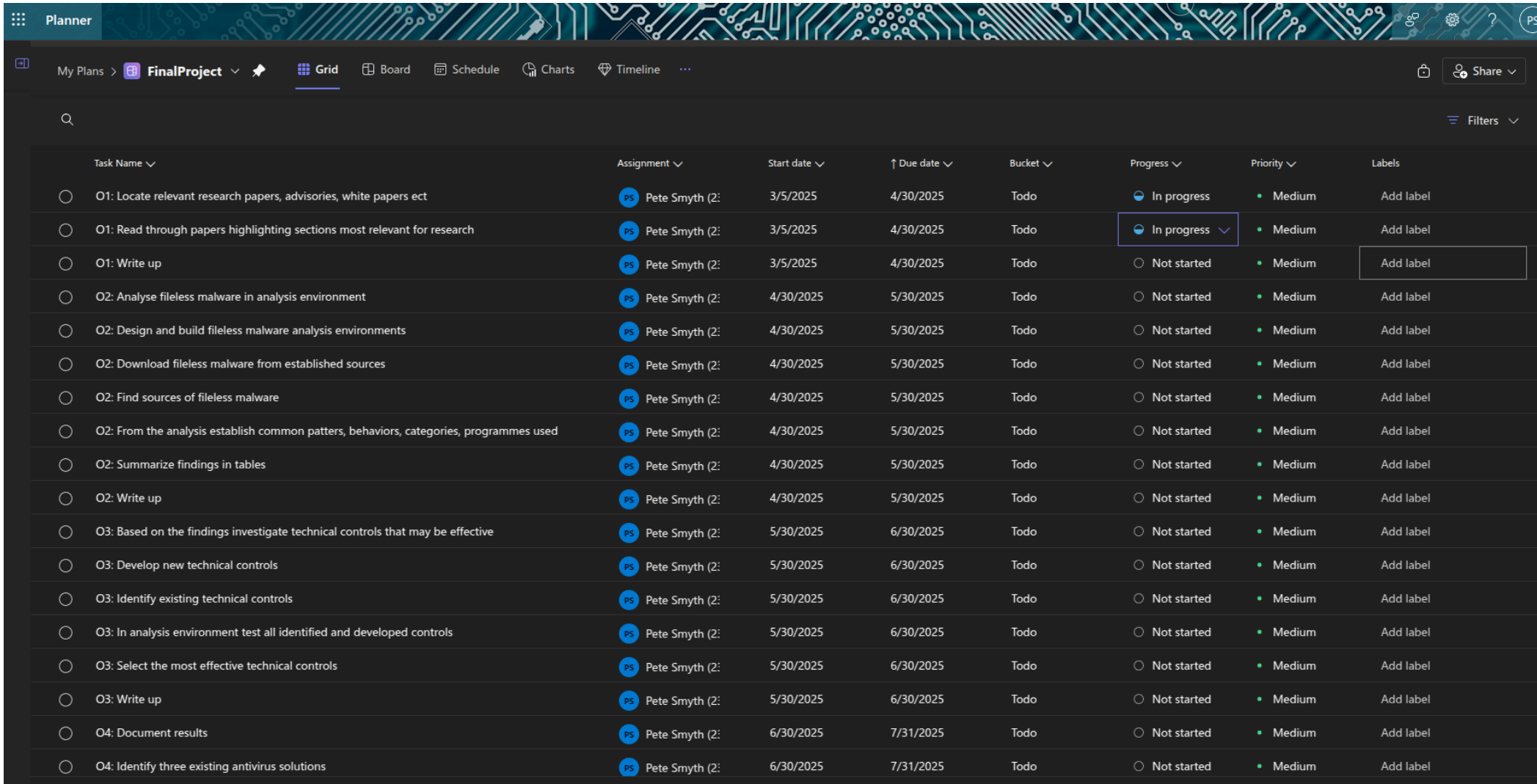
Test identified and developed controls



Evaluate identified and developed controls against antivirus solutions

Fig 3. Research process flow diagram

Project planning and resource management



The screenshot displays the Microsoft Planner interface for a project named 'FinalProject'. The view is set to 'Grid'. The table below represents the data shown in the planner.

Task Name	Assignment	Start date	Due date	Bucket	Progress	Priority	Labels
O1: Locate relevant research papers, advisories, white papers ect	Pete Smyth (2)	3/5/2025	4/30/2025	Todo	In progress	Medium	Add label
O1: Read through papers highlighting sections most relevant for research	Pete Smyth (2)	3/5/2025	4/30/2025	Todo	In progress	Medium	Add label
O1: Write up	Pete Smyth (2)	3/5/2025	4/30/2025	Todo	Not started	Medium	Add label
O2: Analyse fileless malware in analysis environment	Pete Smyth (2)	4/30/2025	5/30/2025	Todo	Not started	Medium	Add label
O2: Design and build fileless malware analysis environments	Pete Smyth (2)	4/30/2025	5/30/2025	Todo	Not started	Medium	Add label
O2: Download fileless malware from established sources	Pete Smyth (2)	4/30/2025	5/30/2025	Todo	Not started	Medium	Add label
O2: Find sources of fileless malware	Pete Smyth (2)	4/30/2025	5/30/2025	Todo	Not started	Medium	Add label
O2: From the analysis establish common patters, behaviors, categories, programmes used	Pete Smyth (2)	4/30/2025	5/30/2025	Todo	Not started	Medium	Add label
O2: Summarize findings in tables	Pete Smyth (2)	4/30/2025	5/30/2025	Todo	Not started	Medium	Add label
O2: Write up	Pete Smyth (2)	4/30/2025	5/30/2025	Todo	Not started	Medium	Add label
O3: Based on the findings investigate technical controls that may be effective	Pete Smyth (2)	5/30/2025	6/30/2025	Todo	Not started	Medium	Add label
O3: Develop new technical controls	Pete Smyth (2)	5/30/2025	6/30/2025	Todo	Not started	Medium	Add label
O3: Identify existing technical controls	Pete Smyth (2)	5/30/2025	6/30/2025	Todo	Not started	Medium	Add label
O3: In analysis environment test all identified and developed controls	Pete Smyth (2)	5/30/2025	6/30/2025	Todo	Not started	Medium	Add label
O3: Select the most effective technical controls	Pete Smyth (2)	5/30/2025	6/30/2025	Todo	Not started	Medium	Add label
O3: Write up	Pete Smyth (2)	5/30/2025	6/30/2025	Todo	Not started	Medium	Add label
O4: Document results	Pete Smyth (2)	6/30/2025	7/31/2025	Todo	Not started	Medium	Add label
O4: Identify three existing antivirus solutions	Pete Smyth (2)	6/30/2025	7/31/2025	Todo	Not started	Medium	Add label

Fig 4. Tracking my research project using Microsoft Planner in Microsoft 365

Description of the project’s potential impact and limitations

Contributions
Guidance on using existing technical controls to combat fileless malware
Potentially new technical controls to combat fileless malware
Improved understanding of fileless malware's operation

Table 3. Contributions of the study

In Scope	Out of Scope
Windows Operating Systems: Windows 10 Enterprise, Windows 11 Enterprise, Windows Server 2025 Windows Server 2022	Unix Operating Systems: Linux distributions, Mac Operating Systems
x86 Architecture	ARM
Windows Defender, Windows antivirus, AVG*, Norton Antivirus* Avast*	Checkpoint, Palo Alto Networks, SolarWinds ect..

*Free / Trail editions

Table 4. In Scope and Out of scope areas of study

```
MmsaeDishcx IndtePsych ';&($Velorgan01) (Fangle  
Para$MultifHypnooboglur DrabuUnextd Sudas  
GuitaParaleChucktSpecit Tick2Jaund=Whole$ Koorel  
AurivSaltl:EllevwEnsobicafetnfejlsd RoquiSambar  
Velorgan01) (Fanglette9 '  
torde$SuedeBklorerErectedecayvCitraiDannegPhysi  
SystfBungmo overrcloniuGertid SmoksgraesaPrereel  
Obtetnitro2  
Unde+Decat$AdvenBYieldrColleeBeleavAfskriLagreg  
Velorgan01) (Fanglette9 'Rolan$DelagCFalcihUdal  
FunkpVandeelremenPatriiTolv Ebbes=Ungdo Dekom(  
RezogAfskrwStegem UnuniTaffy NonvwPneumiSartkn  
Diop2Feltm_SpookpKontir Inclo Arvec Pusse Relas  
Eury-PreocFVorti UnfaiPStoltrSolskoGngetcSussiel  
seIFarefdUdsIa=Lever$Krste{MangrP OmstIKonfeDIndik}  
Nedri.SoileCSaxdioIntermKappem EsIiaRealvnBortf
```

Any Questions?