

APPLICATION FOR ETHICAL APPROVAL

In order for research to result in benefit and minimise risk of harm, it must be conducted ethically.

The University follows the OECD Frascati manual definition of **research activity**: “creative work undertaken on a systematic basis in order to increase the stock of knowledge, including knowledge of man, culture and society, and the use of this stock of knowledge to devise new applications”. As such this covers activities undertaken by members of staff, postgraduate research students, and both taught postgraduate and undergraduate students working on dissertations/projects.

The individual undertaking the research activity is known as the “principal researcher”.

This form must be completed and approved prior to undertaking any research activity.

SECTION A: About You (Principal Researcher)

1	Full Name:	Muhammad Waleed
2	Student Number:	2430361
3	Email address:	2430361@student.uwtsd.ac.uk
4	Programme of Study:	MSc Cybersecurity & Digital Forensics
5	Supervisor:	Dr Dipo Dunsin

SECTION B: Internal and External Ethical Guidance Materials

	Please list the core ethical guidance documents that have been referred to during the completion of this form (including any discipline-specific codes of research ethics, location-specific codes of research ethics, and also any specific ethical guidance relating to the proposed methodology). Please tick to confirm that your research proposal adheres to these codes and guidelines. You may add rows to this table if needed.		
1	UWTSD Research Ethics & Integrity Code of Practice		☒
2	UWTSD Research Data Management Policy		☒
3	Trusted Research and Innovation Policy – English		☒
4	UWTSD Export Control Policy (Research & Innovation) (Senate Final) MI_0		☒
5	UWTSD Open Access Policy 2023 2026 Eng v1.2 JD		☒
6	REICoP-July-2022		☒
7	Research Data Management Policy 2022-v2		☒

SECTION C: Details of Research Activity

1	Indicative title:	AI-Enhanced Security Assessment and Forensic Analysis of GraphQL APIs in Drone Fleet Management Systems		
2	Proposed start date:	06-06-2026	Proposed end date:	06-10-2026
	Introduction to the Research (maximum 300 words in each section)			

	Ensure that you write for a <u>Non-Specialist Audience</u> when outlining your response to the three points below: • <i>Purpose of Research Activity</i> • <i>Proposed Research Question</i> • <i>Aims of Research Activity</i> • <i>Objectives of Research Activity</i> Demonstrate, briefly, how <u>Existing Research</u> has informed the proposed activity and explain • <i>What the research activity will add to the body of knowledge</i> • <i>How it addresses an area of importance.</i>
3	Purpose of Research Activity Drone fleet management systems use Application Programming Interfaces (APIs) to exchange information such as user details, flight schedules, drone locations, mission instructions and operational records. GraphQL is a type of API technology that allows applications to request or update specific information through a single interface. Although this flexibility is useful, weaknesses in its implementation may allow unauthorised access, exposure of sensitive information, manipulation of mission data or disruption of services. The purpose of this research is to investigate whether Artificial Intelligence (AI) can improve the identification, prioritisation and explanation of security weaknesses affecting GraphQL APIs in a drone fleet management system. It will also examine how API requests, system logs and security alerts can be analysed to reconstruct the sequence of events following a simulated cyberattack. The research will be conducted entirely within an authorised and controlled laboratory environment. A simulated drone fleet management application and synthetic user, mission and telemetry data will be used. No live drones, real organisations, external systems or personal data will be involved.
4	Research Question How effectively can an AI-enhanced security assessment and forensic analysis approach identify, prioritise and explain GraphQL API attacks in a simulated drone fleet management system when compared with conventional rule-based security testing methods? Effectiveness will be considered in terms of vulnerability-detection coverage, false-positive results, analysis time and the ability to reconstruct an understandable and reliable timeline of simulated security incidents.
5	Aims of Research Activity The main aim is to develop and evaluate a repeatable method for assessing the security of GraphQL APIs used in drone fleet management systems. The research also aims to determine whether AI-assisted analysis can improve the interpretation of security-testing results and system logs without replacing human judgement. It will examine whether AI can recognise suspicious patterns, connect related events and help prioritise findings according to their possible operational impact. A further aim is to establish how evidence from the API and supporting system logs can be collected and analysed to explain what occurred during a simulated attack, which records were affected and which security controls failed. The final aim is to produce practical recommendations for improving API security, monitoring and forensic readiness in similar systems.
6	Objectives of Research Activity The research objectives are to: • Review existing research concerning GraphQL security, AI-assisted vulnerability detection, drone cybersecurity and digital forensics. • Design a controlled drone fleet management test environment containing a GraphQL API and synthetic operational data. • Create authorised test scenarios covering issues such as unauthorised data access, weak access controls, information exposure, malicious input and resource-intensive queries. • Assess the test API using conventional security-testing methods and AI-assisted analysis. • Compare the approaches using measures including detected vulnerabilities, false positives, testing time and severity prioritisation. • Collect relevant API requests, application logs and security alerts while maintaining the integrity of the evidence. • Reconstruct timelines of the simulated incidents and evaluate whether the evidence explains the actions performed and their effects. • Produce security, monitoring and forensic-readiness recommendations based on the findings. All testing will remain limited to the researcher's isolated and authorised laboratory environment.
	Proposed data collection methods (maximum 600 words)

ETHICS FORM – COMPUTING STUDENTS ONLY

	Existing research has established that GraphQL’s flexible query structure may introduce security risks when access controls and limits on complex requests are not correctly implemented. An empirical study of 8,399 GraphQL schemas found that many were potentially exposed to service disruption through complex queries (Wittern et al., 2019). The OWASP GraphQL Security Guidance similarly identifies weak authorisation, insufficient input validation, information exposure and resource-intensive queries as important concerns. Recent research indicates that context-aware and AI-assisted methods may help identify complex or connected GraphQL attacks that conventional tools can miss (Tsai et al., 2025). Drone-forensics research and the NIST Drone Data Set also demonstrate the value of systematically collecting and examining evidence from drones and related systems. However, GraphQL security testing, AI-assisted analysis and drone forensics are commonly examined as separate areas. This research will bring them together within one controlled drone fleet management case study. It will add comparative evidence about the benefits and limitations of AI-assisted assessment and propose a repeatable approach for connecting security findings with forensic timelines. This is important because an insecure management API could affect operational information, mission integrity, system availability and accountability after an incident. The findings may therefore help developers and security teams build systems that are both more secure and easier to investigate..
7	This should describe how you intend to collect data. It should not include a discussion of the theoretical basis for your data collection methods. Please note, that if you intend to collect any audio/video recordings of interviews with participants then these will be are classified as Personal Data under GDPR/DPA2018. If you intend to use these then note this in section H. (this box should expand as you type)

SECTION D: Scope of Research Activity

	Will the research activity include:	YES	NO
1	Use of a questionnaire or similar research instrument?	☐	☒
2	Use of interviews?	☐	☒
3	Use of focus groups?	☐	☒
4	Use of participant diaries?	☐	☒
5	Use of video or audio recording?	☐	☒
6	Use of computer-generated log files?	☒	☐
7	Participant observation with their knowledge?	☐	☒
8	Participant observation without their knowledge?	☐	☒
9	Access to personal or confidential information without the participants' specific consent?	☐	☒
10	Administration of any questions, test stimuli, presentation that may be experienced as physically, mentally or emotionally harmful / offensive?	☐	☒
11	Performance of any acts which may cause embarrassment or affect self-esteem?	☐	☒
12	Investigation of participants involved in illegal activities?	☐	☒
13	Use of procedures that involve deception?	☐	☒
14	Administration of any substance, agent or placebo?	☐	☒
15	Working with live vertebrate animals?	☐	☒
16	Procedures that may have a negative impact on the environment?	☐	☒

ETHICS FORM – COMPUTING STUDENTS ONLY

17	Other primary data collection methods. Please indicate the type of data collection method(s) below.		
	Details of any other primary data collection method: Primary data will be collected through controlled laboratory experiments using a researcher-developed, simulated drone fleet management system with a GraphQL API. The system will contain only synthetic users, drone missions, location information and telemetry data. A predefined set of authorised security-testing scenarios will be conducted, including attempts to access restricted information, submit invalid inputs and generate unusually complex queries. During each experiment, the system will automatically record API requests and responses, application and security logs, alerts, identified vulnerabilities, processing time and system performance. The same scenarios will be assessed using conventional rule-based security tools and an AI-assisted analysis method. The results will be compared using measures such as vulnerability-detection rate, false positives, analysis time, severity classification and accuracy of incident-timeline reconstruction. Where possible, tests will be repeated under consistent conditions to improve reliability. No questionnaires, interviews or observations of people will be conducted. No human participants, live drones, real organisations, external systems or personally identifiable information will be involved. All testing will remain within an isolated and authorised laboratory environment.	☒	☐

If you have ticked NO to every question then the research activity is (ethically) low risk and you may skip section E and continue to section F.

If YES to any question, then no research activity should be undertaken until full ethical approval has been obtained.

SECTION E: Intended Participants

	Who are the intended participants:	YES	NO
1	Students or staff at the University?	☐	☒
2	Adults (over the age of 18 and competent to give consent)?	☐	☒
3	Vulnerable adults?	☐	☒
4	Children and Young People under the age of 18? (Consent from Parent, Carer or Guardian will be required)	☐	☒
5	Prisoners?	☐	☒
6	Young offenders?	☐	☒
7	Those who could be considered to have a particularly dependent relationship with the investigator or a gatekeeper?	☐	☒
8	People engaged in illegal activities?	☐	☒
9	Others. Please indicate the participants below, and specifically any group who may be unable to give consent.		
	Details of any other participant groups: Complete this only if your participants cannot give consent. This includes animals (this box should expand as you type)	☐	☒

	Participant numbers and source Provide an estimate of the expected number of participants. How will you identify participants and how will they be recruited?	
10	How many participants are expected?	0. This research involves no human participants. All testing will be conducted on a self-hosted, simulated drone fleet management application with a GraphQL API, using synthetic data in an

ETHICS FORM – COMPUTING STUDENTS ONLY

		isolated laboratory environment. No individuals will be recruited, observed, surveyed or otherwise involved.
11	Who will the participants be?	Not applicable.
12	How will you identify the participants?	Not applicable.

	Information for participants:	YES	NO	N/A
13	Will you describe the main research procedures to participants in advance, so that they are informed about what to expect?	☐	☐	☒
14	Will you tell participants that their participation is voluntary?	☐	☐	☒
15	Will you obtain written consent for participation?	☐	☐	☒
16	Will you explain to participants that refusal to participate in the research will not affect their treatment or education (if relevant)?	☐	☐	☒
17	If the research is observational, will you ask participants for their consent to being observed?	☐	☐	☒
18	Will you tell participants that they may withdraw from the research at any time and for any reason?	☐	☐	☒
19	With questionnaires, will you give participants the option of omitting questions they do not want to answer?	☐	☐	☒
20	Will you tell participants that their data will be treated with full confidentiality and that, if published, it will not be identifiable as theirs?	☐	☐	☒
21	Will you debrief participants at the end of their participation, in a way appropriate to the type of research undertaken?	☐	☐	☒
22	If NO to any of above questions, please give an explanation			
	All questions above are marked N/A because this research involves no human participants. Therefore, participant consent, withdrawal, debriefing and participant-confidentiality procedures are not applicable. The research will consist entirely of technical security testing conducted by the researcher within an isolated and authorised laboratory environment, using a simulated drone fleet management system, a GraphQL API and synthetic data. No live drones, real organisations or personally identifiable information will be involved.			

	Information for participants:	YES	NO	N/A
24	Will participants be paid?	☐	☐	☒
25	Is specialist electrical or other equipment to be used with participants?	☐	☐	☒
26	Are there any financial or other interests to the investigator or University arising from this study?	☐	☒	☐
27	Will the research activity involve deliberately misleading participants in any way, or the partial or full concealment of the specific study aims?	☐	☐	☒
28	If YES to any question, please provide full details			
	Not applicable. This research involves no human participants. No participants will be paid, no equipment will be used with participants, and no deception or concealment will take place. The researcher has no financial or other interests arising from this study.			

SECTION F: Anticipated Risks

	Outline any anticipated risks that may adversely affect any of the participants, the researchers and/or the University, and the steps that will be taken to address them.
1	Risks to participants

ETHICS FORM – COMPUTING STUDENTS ONLY

	For example: sector-specific health & safety, emotional distress, financial disclosure, physical harm, transfer of personal data, sensitive organisational information. If you have identified in section D that there are no participants then enter N/A and go skip to question 3.	
	Risk to participants: N/A - This research involves no human participants. All testing will be conducted by the researcher within an isolated, self-hosted laboratory environment using a simulated drone fleet management system, a GraphQL API and synthetic data. No individuals will be recruited, observed, surveyed or involved in any capacity.	<i>How you will mitigate the risk to participants:</i> N/A -; No human participants are involved; therefore, there are no participant-related risks requiring mitigation.
2	If research activity may include sensitive, embarrassing or upsetting topics (e.g. sexual activity, drug use) or issues likely to disclose information requiring further action (e.g. criminal activity), give details of the procedures to deal with these issues, including any support/advice (e.g. helpline numbers) to be offered to participants. Note that where applicable, consent procedures should make it clear that if something potentially or actually illegal is discovered in the course of a project, it may need to be disclosed to the proper authorities	
	N/A - This research involves no human participants and does not investigate or disclose sensitive, embarrassing, upsetting or criminal matters relating to any individual. All security testing will be conducted against a self-hosted simulated system within an isolated and authorised laboratory environment. No live drones, real systems, organisations or individuals will be targeted.	
3	Risks to the investigator For example: personal health & safety, physical harm, emotional distress, risk of accusation of harm/impropriety, conflict of interest	
	Risk to the investigator: The main risk to the investigator is the possible misunderstanding of the research activity. Although all security testing will be authorised and conducted in a controlled laboratory, the use of security-testing tools and simulated attack inputs could be misinterpreted if the purpose and boundaries of the research are not clearly documented. A secondary risk is accidental network misconfiguration, which could unintentionally connect the test environment to external systems. There is also a risk that AI-generated findings may contain false positives or inaccurate classifications. A minor physical risk arises from prolonged computer use, including eye strain, back discomfort and repetitive strain injury.	<i>How you will mitigate the risk to the investigator:</i> The research scope, purpose and testing boundaries will be formally documented and approved through the University's ethics process. Supervisor approval will be obtained before practical testing begins. All testing will be limited to an isolated, self-hosted and authorised laboratory containing a simulated drone fleet management system with a GraphQL API and synthetic data. The environment will operate within dedicated virtual machines using host-only or internal networking. Network settings will be verified before every testing session to prevent interaction with external systems. AI-generated findings will be treated as supporting evidence rather than final conclusions and will be manually validated by the researcher using system logs and conventional security-testing results. Regular breaks, suitable workstation positioning and appropriate screen settings will be used to reduce risks associated with prolonged computer use.
4	University/institutional risks For example: adverse publicity, financial loss, data protection	
	Risk to the University: The main institutional risk is reputational or legal harm if the research is conducted outside its approved scope or is perceived as unauthorised security testing. Accidental interaction with an external or third-party system could create legal, ethical and reputational concerns. There is also a limited data-protection risk if real or personally	<i>How you will mitigate the risk to the University:</i> All practical work will remain strictly within the isolated and self-hosted laboratory environment. No live drones, external systems, third-party services or real organisations will be targeted. Only synthetic users, missions, locations and telemetry data will be used. No personal or confidential organisational data will be collected,

ETHICS FORM – COMPUTING STUDENTS ONLY

	identifiable information is unintentionally introduced into the research environment.	processed or stored. The approved research scope and testing boundaries will be followed throughout the project, and any proposed change to the methodology will be discussed with the supervisor before implementation.
5	Environmental risks For example: accidental spillage of pollutants, damage to local ecosystems	
	Risk to the environment: The research involves the use of a standard laptop and a virtual lab environment. There are no chemical substances, physical materials, or field activities involved. The environmental impact is limited to the standard electricity consumption of the computing equipment used during the project.	<i>How you will mitigate the risk to environment:</i> Environmental impact will be minimised by using existing energy-efficient computing equipment, shutting down virtual machines and the laptop when not in use, and avoiding unnecessary repeated or prolonged testing. No physical materials, chemicals or electronic equipment will be disposed of during the research.

SECTION G: Feedback, Consent and Confidentiality

If you have identified in section D that there are no participants then enter skip this section and continue to section H.

1	Feedback What de-briefing and feedback will be provided to participants, how will this be done and when?	
	You don't need to email your participants with your final report. A good alternative is to set up an email address that they will be able to contact for further details or results. <i>(this box should expand as you type)</i>	
2	Informed consent Describe the arrangements to inform potential participants, before providing consent, of what is involved in participating. Describe the arrangements for participants to provide full consent before data collection begins. If gaining consent in this way is inappropriate, explain how consent will be obtained and recorded in accordance with prevailing data protection legislation.	
	If you are using a paper questionnaire then you should have the participants sign an appropriate consent form. These forms will count as personal data and should be noted as such in section J. If you are using an online questionnaire, then you should have a screen before the questions start that acts as a consent form, informing participants that by clicking on the NEXT button they are providing consent. <i>(this box should expand as you type)</i>	
3	Confidentiality / Anonymity Set out how anonymity of participants and confidentiality will be ensured in any outputs. If anonymity is not being offered, explain why this is the case.	
	Do not collect names unless you really need them. Do not name participants or organisations in any research publications (including the thesis) without their explicit permission. <i>(this box should expand as you type)</i>	

SECTION H: Data Protection and Storage

	Does the research activity involve personal data (as defined by the General Data Protection Regulation 2016 "GDPR" and the Data Protection Act 2018 "DPA")?	YES	NO
1	"Personal data" means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Any	☐	☒

ETHICS FORM – COMPUTING STUDENTS ONLY

	video or audio recordings of participants is considered to be personal data.		
	If YES, provide a description of the data and explain why this data needs to be collected:		
2	This includes audio/video data of participants, but can also include IP addresses and usernames. Names, addresses and emails also count, as do consent forms. (this box should expand as you type)		
	Does it involve special category data (as defined by the GDPR)?	YES	NO
3	“Special category data” means sensitive personal data consisting of information as to the data subjects’ – (a) racial or ethnic origin, (b) political opinions, (c) religious beliefs or other beliefs of a similar nature, (d) membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) physical or mental health or condition, (f) sexual life, (g) genetics, (h) biometric data (as used for ID purposes),	☐	☒
	If YES, provide a description of the special category data and explain why this data needs to be collected:		
4	N/A - No sensitive or special-category personal data will be collected.		

	Will data from the research activity (collected data, drafts of the thesis, or materials for publication) be stored in any of the following ways?	YES	NO
5	Manual files (i.e. in paper form)?	☐	☒
6	University computers?	☒	☐
7	Private company computers?	☐	☒
8	Home or other personal computers?	☒	☐
9	Laptop computers/ CDs/ Portable disk-drives/ memory sticks?	☒	☐
10	“Cloud” storage or websites?	☒	☐
11	Other – specify:	☐	☒
12	For all stored data, explain the measures in place to ensure the security of the data collected, data confidentiality, including details of backup procedures, password protection, encryption, anonymisation and pseudonymisation:		
	All research data, including security scan reports, GraphQL API request and response logs, application and security logs, network traffic captures, screenshots, evaluation results and dissertation drafts, will be generated within an authorised and isolated laboratory environment. Only synthetic data will be used; therefore, no personal, confidential or special-category data will be collected. The primary copy will be stored in the University’s approved Microsoft Office 365 OneDrive environment and will be accessible only through the researcher’s password-protected University account with two-factor authentication enabled. An encrypted backup will be maintained on the researcher’s password-protected personal laptop, which is secured using BitLocker full-disk encryption. If a portable USB drive is required, it will be password-protected and encrypted. Any temporary copies will be securely deleted when no longer required. The data will not be shared with external individuals or organisations and will be retained and securely deleted in accordance with University policy. Anonymisation and pseudonymisation are not required because the research uses only synthetic data and computer-generated laboratory records.		

ETHICS FORM – COMPUTING STUDENTS ONLY

Data Protection			
	Will the research activity involve any of the following activities:	YES	NO
13	Electronic transfer of data in any form?	☒	☐
14	Sharing of data with others at the University outside of the immediate research team?	☐	☒
15	Sharing of data with other organisations?	☐	☒
16	Export of data outside the UK or importing of data from outside the UK?	☐	☒
17	Use of personal addresses, postcodes, faxes, emails or telephone numbers?	☐	☒
18	Publication of data that might allow identification of individuals?	☐	☒
19	If YES to any question, please provide full details, explaining how this will be conducted in accordance with the GDPR and Data Protection Act (2018) (and/or any international equivalent):		
	Question 13 - Electronic transfer will occur between the researcher's password-protected personal laptop and the University-approved Microsoft Office 365 OneDrive account. The transferred files may include GraphQL API logs, security-testing outputs, network captures, screenshots, evaluation results and dissertation drafts. Transfers will use secure encrypted connections, and access will be restricted through password protection and multi-factor authentication. Only synthetic and computer-generated laboratory data will be transferred; no personal, confidential or special-category data will be included. No research data will be intentionally transferred to external organisations or exported outside the UK. All data will be managed in accordance with University data-management and information-security policies.		
20	List all who will have access to the data generated by the research activity:		
	- The student researcher — full access to the laboratory data and research outputs. - The project supervisor — access to relevant technical results, summary findings and dissertation drafts for academic supervision and feedback. - Authorised University markers or examiners — access to the final submitted dissertation and supporting material where required under standard University assessment procedures. No external organisation or unauthorised third party will have access to the raw research data.		
21	List who will have control of, and act as custodian(s) for, data generated by the research activity:		
	The student researcher will act as the primary custodian and will control the day-to-day storage, organisation, protection and deletion of the research data throughout the project. The project supervisor will provide academic oversight. Data stored within the University's Office 365 environment will also remain subject to University data-management, retention and information-security policies.		
22	Give details of data storage arrangements, including security measures in place to protect the data, where data will be stored, how long for, and in what form.		
	All research data will be stored primarily in the University-approved Microsoft Office 365 OneDrive environment and accessed through the researcher's password-protected University account with multi-factor authentication. Temporary working copies may be stored on the researcher's password-protected personal laptop, which is protected by BitLocker full-disk encryption. These files will be synchronised with OneDrive and securely deleted from the laptop when no longer required. If a portable USB drive is essential, it will be encrypted and securely erased after use. The data will be retained in digital form only and may include synthetic drone and mission data, GraphQL API requests and responses, application and security logs, network captures, scan results, screenshots, evaluation results and dissertation drafts. No personal or special-category data will be collected, and no paper copies will be created. All data will be retained until the research has been completed, the dissertation has been assessed, the final award has been confirmed, and any applicable academic review or appeal period has ended. It will then be securely deleted unless a longer retention period is required by UWTSD		

ETHICS FORM – COMPUTING STUDENTS ONLY

	policy. Any data underpinning a publication will be retained in accordance with the applicable University retention requirements.	
22	Confirm that you have read the UWTSD guidance on data management (see https://www.uwtسد.ac.uk/library/research-data-management/)	☒
23	Confirm that you are aware that you need to keep all data until after your research has completed or the end of your funding	☒

SECTION I: Use of AI tools

Use of generative AI and other AI-based tools There are a number of ethical issues relating to the use of generative AI and other AI-based tools, including data security, output bias, and output errors. In general you should assume that any generative AI or other AI-based tool that you pay to use is more secure and accurate than one which is free to use.				
		YES	NO	N/A
Will the research use AI tools to do any of the following:				
1	Capture data?	☐	☒	☐
2	Generate and/or edit text?	☒	☐	☐
3	Generate graphics?	☐	☒	☐
4	Generate video?	☐	☒	☐
5	Generate sound/music?	☐	☒	☐
6	Generate code?	☐	☒	☐
7	Generate synthetic data?	☐	☒	☐
8	Analyse data?	☒	☐	☐
9	Analyse personal or sensitive data?	☐	☒	☐
10	Classify data?	☒	☐	☐
11	Do you intend to use the free version of any AI tools?	☒	☐	☐
If you have answered YES to any of questions O1-O11, please provide justification detailing why this is necessary for the research.				
12	A locally hosted AI-based tool will be used to analyse and classify computer-generated security data from the simulated GraphQL API environment. The inputs will include synthetic API requests and responses, application and security logs, scan findings, alerts and system-performance records. The AI tool will assist in identifying suspicious patterns, prioritising findings and producing technical explanations and reconstructed incident timelines for evaluation. The use of AI is necessary because the research aims to compare an AI-enhanced security and forensic analysis approach with conventional rule-based security-testing methods. AI outputs will be evaluated using measures including detection coverage, false-positive results, analysis time, severity classification and incident-timeline accuracy. All processing will take place within the researcher's isolated and authorised laboratory environment. No personal, sensitive or confidential data, live-drone data, or information belonging to a real organisation will be processed. AI-generated outputs may contain errors or false positives; therefore, every finding will be manually validated using conventional security-testing results and original system logs. The AI tool will support, rather than replace, the researcher's judgement.			

SECTION J: Declaration

	The information which I have provided is correct and complete to the best of my knowledge. I have attempted to identify any risks and issues related to the research activity and acknowledge my obligations and the rights of the participants. In submitting this application I hereby confirm that I undertake to ensure that the above named research activity will meet the University's Research Ethics and Integrity Code of Practice which is published on the website: https://www.uwtsd.ac.uk/research/research-ethics/		
1	Signature of applicant:	Muhammad Waleed	Date: 10-08-2026
2	Supervisor:	Dr Dipo Dunsin	Date:
3	Signature:	D Dunsin	