COMP3010
Security Operations & Incident Management

20 CREDIT MODULE

ASSESSMENT: 100% Coursework	**W1: 30% Report Outline** **W2: 70% Report**

MODULE LEADER: Dr Ji-Jian Chin

MODULE AIMS

- To design and develop organisational security operations and incident management architectures that provide a holistic solution to enabling situational awareness and incident management
- To introduce roles, methodologies and practices underpinning incident management and the creation of Computer Security Incident Response Teams (CSIRTs)
- To introduce the range of techniques that will allow an Intrusion Analyst to intelligently examine network traffic for signs of intrusions and respond to computer incidents.

ASSESSED LEARNING OUTCOMES (ALO):

1. Illustrate the structure, roles and responsibilities of a security operations centre.
2. Design and develop technical infrastructures for the management and monitoring of cyber security.
3. Undertake analysis of data and select appropriate intrusion analysis methodologies to analyse intrusion alarms.

Overview

This document contains all the necessary information pertaining to the coursework of *COMP3010 Security Operations & Incident Management*. The module is assessed via **100% coursework**, across two elements: *30% Set Exercises* and *70% Report*.

The sections that follow will detail the coursework tasks that are to be undertaken. The submission and expected feedback dates are presented in Table 1. All courseworks are to be submitted electronically via the respective DLE module pages before the stated deadlines.

	Submission Deadline	Feedback
Coursework 1 (30%)	**3th November 2025 (15:00)**	**2nd December 2025 (15:00)**
Coursework 2 (70%)	**9th January 2026 (15:00)**	**9th February 2026 (15:00)**

Table 1: Coursework Deadlines

All courseworks will be introduced in class to provide further clarity over what is expected and how you can access support and formative feedback prior to submission. **Whilst the coursework information is provided at the start of the module, it is not necessarily expected you will start this immediately** – as you will often not have sufficient understanding of the topic. The module leader will provide guidance in this respect.

Moderation

This assignment brief has been moderated in line with the university policy.

Moderator Name	**Moderation Date**
Hai-Van Dang	3 October 2025

Useful Assignment Information

Please see below some useful information regarding submissions for your modules.

Good Coding Practices

Like all things, no code is perfect. Just because your code compiles and runs does not mean it is perfect, there is always room for improvement. No code will achieve 100% of the available marks. Where code submission is required by a module, it will be assessed against the following criteria:

1) **Functionality**
    a. Does your code meet all the specified requirements of the assignment?
    b. Does your code behave correctly across typical and edge-case scenarios?
    c. Does you code have appropriate error handling that does not leading to it crashing or undefined behaviour?
2) **Efficiency**
    a. Is your code optimised in terms of performance and resource use?
    b. Does you code handle functions, variables, data calls efficiently?
    c. Is there any unnecessary repetition, complexity or processing reducing efficiency within your code?
3) **Readability**
    a. Is your code logically structured and easy to read?
    b. Have you maintained standard formatting conventions like indentations, spacing and naming, within your code?
    c. Are variables, functions, and classes clearly named and purposeful?
4) **Documentation**
    a. Are there helpful comments explaining non-obvious parts of your code?
    b. Do your comments document your process, development or rationale clearly?
    c. Could someone unfamiliar with the code understand the approach you have taken?

Use of Generative AI for Creating Code

Each assignment element for each module will have a clear indication of the permitted level of use of AI (solo, assisted or partnered) including the generation of code. Please ensure that you **read and understand the permitted use**. If you are unsure of a particular use, please reach out to the Module Leader and ask.

We strongly encourage you to read and explore beyond the core content delivered within the modules. However, this must be done correctly following academic process. Wherever code is drawn from an outside source (e.g. you have not written it yourself), regardless of whether this is AI generated or from an online repository (GitHub, Stack Overflow etc) **you must reference the original source**. This can be done in your documentation as comments or part of your write ups. Students found to be utilising code without referencing could face an academic offence. **If in doubt speak to your Module Leader.**

Versioning

A critical part of a development (software or academic) is versioning. Keeping a number of iterations over the course of development ensures you always have backups to fall back on. It also provides clear demonstration of the development process you implemented.

Using online/cloud-based storage solutions and repositories provide additional peace of mind, alongside being industry practice. The university provide OneDrive to all students which offers inbuilt version history for Microsoft products. GitHub is the university recommended repository for versioning code, which includes great integration with a number of IDEs.

Submitting Code

It is vital that you confirm that all code that you submit is in the **correct format** and **compiles correctly** or **runs without error**. If you clean up your code before submission, please ensure that all dependencies (libraries, functions and variables) are included so that the marker can compile your code.

We can only mark what has been submitted. If the code does not run correctly, it is not our responsibility to spend time error handling to award you marks.

It is also important to **show your working**. Tidying up your code is a critical part of coding practices, but if you remove the workings that provides you with the required output, we cannot see how you got there.

In a worst-case scenario, if you remove a key part of your working, and on compiling your code it gives an error or different result, we have no way of confirming what went wrong, or indeed if you fabricated those outputs.

Please note, just because a piece of code has given the wrong output, it does not mean it should be deleted. Seeing these attempts with comments documenting your attempt allows us to understand where you may have made an error and provide feedback that addresses this. In some cases, you could also be awarded marks for the attempt.

Coursework 1: Set Exercises - PCAP Analysis

Task:

The Set Exercises in this module are focused on undertaking and analysing several experimental based lab exercises. Within the module plan, several laboratory exercises provide a better understanding of the capability of incident detection and management tools. These include:

- Effectiveness of different network intrusion/monitoring tools
- Gathering information for an incident report
- Exploration of pcap packets for evidence
- Investigating alerts for intruders

You work as a security analyst. One day you receive the following pcap file with an intrusion incident detected. You are required to perform a detailed intrusion analysis on the provided network traffic logs. A set of questions have been prepared to aid you in your analysis. You will find them on as a quiz on the DLE. Using the answers from the questions in the quiz (separate document), write a 1000-word report on your findings, detailing the following:

- **Identify the Infected System:** Detect which system in the network has been compromised.
- **Analyse How the Infection Occurred:** Determine the method used to infect the system.
- **Identify the Type of Infection**: Describe what type of malware or attack caused the infection.

Important Notes:

- This is **individual work** and **not** a textbook-based exercise.
- You are expected to conduct a practical experiment, document your process, analyse the results, and produce an incident report.
- Your report should focus on the **application of knowledge** rather than merely presenting theoretical or textbook information. Critical analysis and thorough documentation of your investigative process are key to this assignment.

Submission Requirements:

- Provide answers on DLE quiz.
- 1000-word limit incident writeup, inclusive of evidence. Writeup submitted at as single PDF document to DLE.
- Include appendix with completed Generative AI Declaration (not part of word limit).
- Optional: Replicate on a public Github for showcase.
- Optional: Video walkthrough (10 minutes) for better marks on evidence.

Coursework Criteria:

The recommended structure for incident writeup is as specified in the following table. Please be very careful and pay close attention to these instructions in table 1.

Content	Details
Section 1 - Introduction	What you are covering and why, how the report is structured
Section 2 – Methodology	**Methodology**: What are the tools to be used for the intrusion analysis? Explain how you perform the intrusion analysis to identify the infected system information (IP address, MAC address, hostname, user account name of the infected machine), an indicator of the infection, and how the system got infected. **Please provide screenshots of the analysis using appropriate tool(s), inputs, and outputs to evidence the application of knowledge.**

Section 3 - Results	Present and explain the results. Use the answers to the quiz questions to guide your writeup. **Please provide screenshots of the results as evidence.**
Section 4 - Conclusion & References	Conclude with prevention techniques on how you can prevent such future incidents in the report. Discuss any relevant open issues/ challenges.

Table 2: Coursework 1 structure

Question Set for Coursework 1: (provide your answers on the DLE quiz)
(2 marks each question. Provide evidence in writeup.)

Part 1: Initial Infection & File Transfer

1. When did the initial malicious HTTP connection occur? (Provide the date and time in yyyy-mm-dd hh:mm:ss format).
2. What is the name of the compressed file that the victim downloaded?
3. Which domain hosted the malicious compressed file?
4. What is the name of the file located inside the compressed archive?
5. Identify the specific web server software (Server header) running on the malicious IP address that served the compressed file.
6. What is the version number of the web server identified in the previous question?
7. Identify the three additional domains that were involved in downloading malicious files to the victim host.
   Hint: Inspect HTTPS traffic and focus on the time window between 16:45:11 and 16:45:30. Note this range is in UTC, not BST.

Part 2: Command and Control (C2) Activity

8. Which Certificate Authority (CA) issued the SSL certificate for the first domain identified in question 7?
9. What are the two IP addresses of the Cobalt Strike servers? (Provide them in sequential order).
   Hint: Inspect the Conversations menu option
10. What is the value of the Host header for the first Cobalt Strike IP address?
    Hint: Apply a filter to isolate DNS queries.
11. What is the domain name associated with the first Cobalt Strike IP address?
    Hint: Take a closer look at HTTPS (443)
12. What is the domain name associated with the second Cobalt Strike IP address?
    Hint: Apply a filter to capture HTTP POST requests.
13. What is the domain name used for the post-infection traffic?
14. What are the first eleven characters of the data the victim host sends to the malicious domain identified in the previous question?
15. What was the length of the first packet the victim sent to the C2 server?
16. What was the Server header value for the malicious domain from question 13?

Part 3: Final Exfiltration/Check-in

17. What was the date and time (in yyyy-mm-dd hh:mm:ss UTC format) when the DNS query occurred for the domain used by the malware to check the victim's external IP address?

18. What was the domain name in the DNS query from the previous question?
19. What was the first email address observed in the SMTP traffic in the pcap file (the MAIL FROM address)?
20. Follow the stream from Q19. What is *ho3ein.sharifi's* password?

Acceptable level of generative AI tool use in this coursework element

Partnered Work	Generative AI tool use is required as an integral part of the coursework, but transparency is required.	☒

Table 3: Acceptable Level of generative AI use

Any use of AI in your work must be declared within your documentation. You **must also include a signed Generative AI Declaration as an appendix to your submission**. The declaration form can be found on DLE (or Here on the Programme Page). This form will not be included in any word count associated with this assignment.

The report must not exceed 1000 words or 10 pages (whichever shorter) excluding screenshots and references. Please note that anything exceeding the maximum number of pages will not be accessed by the markers. A Rubric will be used to assess and provide feedback. The template for this can be found below (Table 2).

Threshold Criteria (these are indicative only):

To achieve 40%+ (Pass):

Students must complete the quiz with some correct answers and provide a minimally structured incident report. Basic evidence (e.g., a screenshot) should be included to demonstrate that an experiment was attempted. Limited analysis is acceptable, but there must be a clear attempt to link findings to the incident.

To achieve 50%+ (Merit – lower):

Students must answer the majority of quiz questions correctly, showing reasonable understanding of the incident. The report should present a clear methodology with appropriate tools and data and provide coherent results. Evidence should support key claims, though integration may be limited. Some reflection on incident impact should be present.

To achieve 60%+ (Merit – upper):

Students must demonstrate a strong understanding in the quiz with most answers correct and explained. The incident report should be well-structured, with a reliable methodology, strong analysis of results, and clear interpretation of how the infection occurred. Evidence must be relevant, clearly presented, and support the report findings. References and critical comparison with prior knowledge of the domain are expected.

To achieve 70%+ (Distinction):

Students must achieve an excellent standard across all components: full or near-full quiz answers with insightful reasoning, a professional incident report with outstanding structure and depth of analysis, and comprehensive evidence fully integrated with the writeup. The report should demonstrate critical reflection, awareness of wider implications, and forward-looking recommendations. Work should align with professional security practice and academic standards, with high-quality referencing where relevant.

Criteria	Fail (<40%)	Pass (40%+)	Merit (60%+)	Distinction (70%+)	Grade
Answering the questions	Each question is assigned a weight. The sum of all questions will contribute 40% to the total of this coursework.				/40
Incident Writeup	Report incomplete, poorly structured, or irrelevant. No meaningful methodology or analysis. Answers from quiz ignored or copied without reflection.	Report covers minimum required sections (Intro, Methodology, Results, Conclusion). Structure present but weak. Analysis limited to surface-level restatement of quiz answers.	Report well-structured and coherent. Appropriate methodology explained. Clear analysis of results, with logical interpretation of how infection occurred. Discussion of impact present.	Professional-level report with excellent structure and depth of analysis. Methodology and reasoning are precise and well-documented. Clear narrative linking evidence, quiz answers, and incident interpretation. Reflection on wider implications included.	/30
Evidence	No screenshots or evidence provided. Evidence irrelevant, copied or fabricated.	Minimal evidence provided (e.g., 1–2 screenshots). Screenshots only loosely connected to analysis.	Relevant screenshots or outputs provided. Evidence clearly supports results. Some integration into narrative.	Comprehensive, well-chosen evidence (screenshots, logs, tool outputs). Evidence fully integrated into the analysis with annotations. Demonstrates hands-on application and professional reporting standards. Inclusion of video evidence.	/30
Feedback/ Overall	*Additional feedback*				**/100**

Table 4: CW1 Marking Rubrics

Coursework 2: BOTSv3 Incident Analysis and Presentation

Task

BOTSV3, or Boss of the SOC (BOTS) Dataset Version 3, is a publicly available, pre-indexed sample security dataset and Capture The Flag (CTF) platform created by Splunk to train and test the skills of cybersecurity professionals, students, and enthusiasts. It simulates a realistic security incident within a fictitious brewing company named "Frothly," providing a massive collection of logs—including network, endpoint, email, and cloud service data from environments like Amazon AWS and Microsoft Azure—which participants must analyze using Splunk's Search Processing Language (SPL) to investigate the simulated attack and answer specific questions following the cyber kill chain methodology.

In this coursework, you will work individually to investigate and report on security incidents using the **Boss of the SOC v3 (BOTSv3)** dataset within **Splunk**. To begin, go to https://github.com/splunk/botsv3 to retrieve the dataset. You will need to set up your own Splunk on Ubuntu VM, then follow the instructions on the botsv3 repo to ingest the dataset.

Your deliverables are:

1. A **public GitHub repository** containing a README.md file written as your professional report.
2. A **YouTube video presentation** (max 10 minutes) embedded/linked in the GitHub repository.
3. Evidence of **continuous improvement** on your GitHub repo across at least two weeks, shown by commit frequency and timestamps.

This format reflects industry practice, where professionals document security investigations publicly or internally using markdown and version control.

Acceptable level of generative AI tool use in this coursework element

Partnered Work	Generative AI tool use is required as an integral part of the coursework, but transparency is required.	☒

Table 5: Acceptable Level of generative AI use

Report Structure and Key Sections

Your written report should follow this structure:

- **Introduction (10%)**
  Provide an overview of the SOC context, the BOTSv3 exercise, and the objectives of your investigation. Clearly define scope and assumptions.
- **SOC Roles & Incident Handling Reflection (10%)**
  Reflect on how SOC tiers, responsibilities, and incident handling methodologies relate to the BOTSv3 exercise. Discuss prevention, detection, response, and recovery phases.
- **Installation & Data Preparation (15%)**
  Document Splunk installation, dataset ingestion, and validation steps. Provide supporting evidence (screenshots/configs). Justify setup choices in the context of SOC infrastructure.
- **Guided Questions (40%)**
  Choose and answer **<u>ONE SET</u>** of BOTSv3's 200-level questions using Splunk queries and analysis. Present answers clearly, with supporting evidence (screenshots, query outputs, dashboards). Explain the SOC relevance of each answer.

- **Conclusion, References and Presentation (5%)**
  Summarise findings, key lessons, and SOC strategy implications. Highlight improvements for detection and response.
- Professionally structured, correctly referenced (IEEE style), and clearly written. You may use Zotero or EndNote to help you.

Evidence Presentation – Video Presentation and Continuous Github Improvements (20%)

In addition to the report, you must prepare a maximum **10 minute recorded presentation** that:

- Summarises your key findings from BOTSv3.
- Demonstrates selected Splunk queries/dashboards.
- Reflects on SOC operations and incident response lessons learned.
- Is clear, professional, and suitable for a security management audience.

Additionally, there should be evidence of continuous work being done in a span of at least 4 weeks evidenced in Github pushes to show progress.

Key Expectations

- Demonstrate deep understanding of SOC structures, roles, and responsibilities.
- Show practical Splunk analysis with accurate answers to BOTSv3 questions.
- Present evidence of critical reflection on SOC practices and incident handling.
- Use GitHub for professional technical documentation and continuous improvement.
- Deliver findings clearly in both README.md and video presentation.

Report Guidelines:

- Submission format: Public GitHub repository with a README.md as the report.
- Word count: max 2,000 words (excluding appendices/screenshots).
- Video length: max 10 minutes, YouTube unlisted link embedded in repo.
- Continuous improvement: Repo must show commit activity across at least 4 weeks.

Submission Requirements:

- Provide answers on DLE quiz.
- 2000-word limit incident writeup, inclusive of evidence. Writeup submitted at as single PDF document to DLE.
- Include appendix with completed Generative AI Declaration (not part of word limit).
- Video walkthrough (max 10 minutes).
- Replicate on a public Github for showcase. Continuous commits for 4 weeks prior to deadline (not including holidays)

Question set for Coursework 2 (provide your answers on the DLE quiz)

In this task, you'll focus on AWS-related events with some questions focusing on endpoint-related events. Provide answers on the DLE, but include evidence in your report.

Question	Details	Marks
1	You're tasked to find the IAM (Identity & Access Management) users that accessed an AWS service in Frothly's AWS environment. Refer to the following link to get an idea of what source type you need to query and what field in the results will have the answer you're seeking.	5

	Link: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-examples.html List out the IAM users that accessed an AWS service (successfully or unsuccessfully) in Frothly's AWS environment? Answer guidance: Comma separated without spaces, in alphabetical order. (Example: ajackson,mjones,tmiller) *Hint: Use aws:cloudtrail as the source type.*	
2	The following links are provided to help you with this question. Links: • https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-public-access/ • https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail-additional-examples.html#cloudwatch-alarms-for-cloudtrail-no-mfa-example Make sure you exclude events related to console logins. It might be a good idea to do a keyword search query on this one. Don't forget to surround the keyword with asterisks. What field would you use to alert that AWS API activity has occurred without MFA (multi-factor authentication)? Answer guidance: Provide the full JSON path. (Example: iceCream.flavors.traditional) *Hint: Use aws:cloudtrail as the source type.*	5
3	Look at the source types available in the dataset. There might be one in particular that holds information on hardware, such as processors. What is the processor number used on the web servers? Answer guidance: Include any special characters/punctuation. (Example: The processor number for Intel Core i7-8650U is i7-8650U.) *Hint: Use hardware as the source type in Splunk Search for find hardware information such as CPU statistics, hard drives, network interface cards, memory, and more.*	5
4	Questions 4-6: A common misconfiguration involving AWS is publically accessible S3 buckets. Read the following resource to understand ACLs and S3 buckets. Link: https://docs.aws.amazon.com/AmazonS3/latest/API/API_PutBucketAcl.html Question 4: Bud accidentally makes an S3 bucket publicly accessible. What is the event ID of the API call that enabled public access? Answer guidance: Include any special characters/punctuation. *Hint: Use aws:cloudtrail as the source type to search for the PutBucketAcl event.*	5

5	What is Bud's username?	5
6	What is the name of the S3 bucket that was made publicly accessible? *Hint: Use aws:cloudtrail as the source type.*	5
7	You're tasked with identifying a text file uploaded to the S3 bucket. Here is a link for more information related to this topic. Link: https://docs.aws.amazon.com/AmazonS3/latest/API/API_PutObject.html Since you know the *name* of the S3 *bucket*, you should easily find the answer to this question. You will need to query a different AWS-related source type. HTTP status code might be helpful as well. What is the name of the text file that was successfully uploaded into the S3 bucket while it was publicly accessible? Answer guidance: Provide just the file name and extension, not the full path. (Example: filename.docx instead of /mylogs/web/filename.docx) *Hint: Use aws:s3:accesslogs.*	5
8	What keywords can you start your search with to help identify what data sources can help you with this? One of the fields within this source type clearly has the answer, but which is it? Perhaps expanding upon your search to count on the operating systems and hosts will be helpful. What is the FQDN of the endpoint that is running a different Windows operating system edition than the others? *Hint: Start with winhostmon as the source type.*	5

Refer to Table 3 for a detailed breakdown of how your work will be assessed.

40%+ (Pass):

- Demonstrates basic understanding of Splunk setup and dataset ingestion.
- Able to run simple queries to answer a few 200-level BOTSv3 questions.
- Evidence is minimal or incomplete (e.g., screenshots/configurations missing or unclear).
- Shows limited awareness of SOC roles and responsibilities, but some recognition of incident handling steps.
- GitHub repository contains a basic README.md with minimal structure or referencing; commit history shows little continuous improvement.
- Video presentation provides only a brief summary of activities with weak structure or clarity.
- Overall submission meets baseline technical expectations but lacks analytical depth or professional presentation.

50%+ (Merit – Lower):

- Demonstrates good understanding of Splunk installation, dataset ingestion, and BOTSv3 analysis workflow.
- Provides accurate answers to most 200-level questions, supported by evidence (queries, screenshots).
- Shows a reasonable understanding of SOC roles, responsibilities, and incident handling methodologies.
- README.md report is clear and readable, includes basic references, and follows a logical structure.
- GitHub repository shows some evidence of progressive improvement, though commits may be irregular.
- Video presentation clearly explains findings and workflow but lacks full professional polish or depth.
- Overall submission reflects developing analytical skill and technical competence consistent with early SOC practitioner level.

60%+ (Merit – Upper):

- Demonstrates very good understanding of Splunk installation, dataset preparation, and investigative workflow within the BOTSv3 environment.
- Accurately answers almost all 200-level questions, supported by clear, justified methodologies and appropriate evidence.
- Integrates understanding of SOC responsibilities, technical infrastructures, and intrusion analysis into a coherent, well-structured report.
- README.md demonstrates professional writing, consistent referencing, and logical organisation of content.
- GitHub repository shows regular commits across at least two weeks, demonstrating continuous improvement and reflection.
- Video presentation is well-structured and professional, clearly highlighting key investigative findings and lessons learned.
- Overall, the submission shows strong analytical reasoning and solid professional communication, linking technical findings to SOC practice.

70%+ (Distinction):

- Demonstrates excellent understanding of SOC structures, Splunk-based analysis, and end-to-end BOTSv3 investigation.
- Provides complete, well-justified answers to all 200-level questions, supported by comprehensive evidence (queries, dashboards, outputs, reflections).
- Offers critical reflection on SOC processes, escalation paths, and strategic incident handling methodologies, showing mastery of applied cybersecurity practice.
- Includes critical comparison of tools and techniques, with insightful, forward-looking recommendations for SOC improvement.
- GitHub repository exhibits excellent professional practice — frequent, meaningful commits; a high-quality README.md with integrated video, IEEE references, and coherent structure.
- Video presentation is of professional standard — engaging, insightful, and demonstrating strategic thinking beyond technical findings.
- Overall submission showcases the ability to synthesize technical expertise, SOC awareness, and professional communication consistent with industry-level performance.

Criteria	Fail (<40%)	Pass (40–49%)	Merit (50–59%)	Merit (60–69%)	Distinction (70%+)	Weight
Introduction	No clear introduction, objectives missing.	Basic intro with vague scope.	Adequate intro with some SOC context.	Clear, structured intro with defined scope.	Professional, insightful intro; strong SOC contextualisation.	10%
SOC Roles & Incident Handling Reflection	No reference to SOC processes.	Minimal discussion of SOC responsibilities.	Some understanding of SOC roles and incident handling methodologies.	Good explanation of SOC roles, escalation, and response processes linked to findings.	Excellent critical reflection on SOC structures and methodologies; professional-level insight.	10%
Installation & Data Preparation	No evidence of Splunk setup or dataset ingestion.	Minimal description of setup, limited screenshots.	Adequate explanation of setup, dataset prepared with partial evidence.	Well-documented installation and ingestion, justified in SOC context.	Comprehensive documentation of Splunk setup with critical justification of design choices.	15%
Guided Questions (BOTSv3 Q&A)	BOTSv3 questions largely unanswered/incorrect.	Answers a few 200-level questions, limited evidence.	Accurate answers to a number of 200-level questions, some evidence provided.	Accurate answers to most 200-level questions, with strong evidence.	Complete, well-justified answers to all 200-level questions, comprehensive evidence and reflection.	40%
Conclusion, References & Professional Presentation	No conclusion or irrelevant. Poor structure, no references, unclear writing.	Weak conclusion with limited connection to findings.	Adequate summary with some lessons learned.	Strong conclusion, clear lessons, SOC reflection.	Professional conclusion with synthesis of findings and forward-looking recommendations.	5%
Video Presentation	No video submitted, or irrelevant content.	Video submitted but weak, poorly structured.	Clear explanation of findings but lacks polish.	Well-structured, professional summary of analysis.	Excellent, professional-quality presentation; clear, engaging, and strategic.	10%
Continuous Improvement (GitHub Commits)	No evidence of ongoing work; single upload only.	Minimal commits with weak timestamps.	Some evidence of continuous improvement, limited frequency.	Regular commits over 2 weeks, clear progress in repo.	Excellent commit history showing continuous development, reflection, and professional repo management.	10%
Total						**100%**

Table 6: Feedback Template for Coursework 2

Acceptable levels of AI use:

The table below provides the acceptable use categories for GenAI. Each Coursework element may allow different uses. Please check the brief for each element carefully to see what uses are allowed.

Solo Work	**S1 - Generative AI tools have not been used for this coursework.**
Assisted Work	**A1 – Idea Generation and Problem Exploration** Used to generate project ideas, explore different approaches to solving a problem, or suggest features for software or systems. Students must critically assess AI-generated suggestions and ensure their own intellectual contributions are central.
	A2 - Planning & Structuring Projects AI may help outline the structure of reports, documentation and projects. The final structure and implementation must be the student's own work.
	A3 – Code Architecture AI tools maybe used to help outline code architecture (e.g. suggesting class hierarchies or module breakdowns). The final code structure must be the student's own work.
	A4 – Research Assistance Used to locate and summarise relevant articles, academic papers, technical documentation, or online resources (e.g. Stack Overflow, GitHub discussions. The interpretation and integration of research into the assignment remain the student's responsibility.
	A5 - Language Refinement Used to check grammar, refine language, improve sentence structure in documentation not code. AI should be used only to provide suggestions for improvement. Students must ensure that the documentation accurately reflects the code and is technically correct.
	A6 – Code Review AI tools can be used to check comments within the code and to suggest improvements to code readability, structure or syntax. AI should be used only to provide suggestions for improvement. Students must ensure that the code accurately reflects their knowledge and is technically correct.
	A7 - Code Generation for Learning Purposes Used to generate example code snippets to understand syntax, explore alternative implementations, or learn new programming paradigms. Students must not submit AI-generated code as their own and must be able to explain how it works.
	A8 - Technical Guidance & Debugging Support AI tools can be used to explain algorithms, programming concepts, or debugging strategies. Students may also help interpret error messages or suggest possible fixes. However, students must write, test, and debug their own code independently and understand all solutions submitted.
	A9 - Testing and Validation Support AI may assist in generating test cases, validating outputs, or suggesting edge cases for software testing. Students are responsible for designing comprehensive test plans and interpreting test results.
	A10 - Data Analysis and Visualization Guidance AI tools can help suggest ways to analyse datasets or visualize results (e.g. recommending chart types or statistical methods). Students must perform the analysis themselves and understand the implications of the results.
	A11 - Other uses not listed above Please specify:
Partnered Work	**P1 - Generative AI tool usage has been used integrally for this coursework** Students can adopt approaches that are compliant with instructions in the coursework brief. Please Specify: • Research further concepts • Write/generate/troubleshoot scripts to facilitate analysis • Report generation and improvements • Readme report, script crafting.

General Guidance

Responsible use of Artificial Intelligence (AI) in courseworks

Please refer to https://dle.plymouth.ac.uk/mod/resource/view.php?id=1657202 for guidelines about what you can use AI and what you cannot use AI for when writing or submitting courseworks.

Extenuating Circumstances

There may be a time during this module when you experience a serious situation that has a significant impact on your ability to complete the courseworks. The definition of these can be found in the University Policy on Extenuating Circumstances here: https://www.plymouth.ac.uk/student-life/your-studies/essential-information/exams/exam-rules-andregulations/extenuating-circumstances

Plagiarism

All of your work must be in your own words. You must use references for your sources; however, you acquire them. Where you wish to use quotations, these must be a very minor part of your overall work.

To copy another person's work is viewed as plagiarism and is not allowed. Any issues of plagiarism and any form of academic dishonesty are treated very seriously. All your work must be your own and other sources must be identified as being theirs, not yours. The copying of another person's work could result in a penalty being invoked.

Further information on plagiarism policy can be found here:

Plagiarism: https://www.plymouth.ac.uk/student-life/your-studies/essentialinformation/regulations/plagiarism

Examination Offences: https://www.plymouth.ac.uk/student-life/your-studies/essentialinformation/exams/exam-rules-and-regulations/examination-offences

Turnitin (http://www.turnitinuk.com/) is an Internet-based 'originality checking tool' that allows documents to be compared with content on the Internet, in journals, and in an archive of previously submitted works. It can help to detect unintentional or deliberate plagiarism.

It is a formative tool that makes it easy for students to review their citations and references as an aid to learning good academic practice. Turnitin produces an 'originality report' to help guide you. To learn more about Turnitin go to:
https://guides.turnitin.com/hc/en-us/categories/21850416398221-Student-hub

Referencing

The University of Plymouth Library has produced an online support referencing guide which is available here: http://plymouth.libguides.com/referencing.

Another recommended referencing resource is Cite Them Right Online; this is an online resource that provides you with specific guidance about how to reference lots of different types of materials.

The Learn Higher Network has also provided a number of documents to support students with referencing:
References and Bibliographies Booklet: http://www.learnhigher.ac.uk/writing-for-university/referencing/references-and-bibliographiesbooklet/
Checking your assignments' references:
http://www.learnhigher.ac.uk/writing-for-university/academic-writing/checking-your-assigmentsreferences/