PUSL3131
Security Operations & Incident Management

20 CREDIT MODULE

ASSESSMENT: 50% Coursework

MODULE LEADER: Dr Hai-Van Dang

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 assessment of *PUSL3131*. The module is assessed via **50% coursework, 50% exam.**

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

	Submission Deadline	Feedback
Mandatory group enrolment on DLE for the coursework	**27 November 2026**	**If not registering to any group, you will not receive the awarded marks.**
Individual Exam (50%)	**TBC**	**Within 20 working days**
Group coursework (50%)	**TBC, 4pm Sri Lanka time (10.30 am UK time)**	**Within 20 working days**

Table 1: Assessment Deadlines

All assessments 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 assessment 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

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 assessment

Task:
This is a **group** coursework, for groups of **FOUR** students and is worth 50% of the total module mark. The students must register the group on DLE. Without the group registration, the students will not be able to submit the report.

An airline company has an online booking system for its customers using both a mobile app as well as a web interface. This system supports the customers to book flights online using their debit/credit cards, submit their personal details etc. Both the mobile app and the web-interface are connected via internet to a back-end server which is also accessible to the admin through a web-interface. The airline company has been made aware of the legal requirements to secure user's' private data and they have put forward security as an essential requirement for this booking system. Unfortunately, recently, the IT team has detected an intrusion. They have recorded the network traffic in *coursework2026.pcap* (the file is provided on DLE). However, they are uncertain how the infection happened and what the infection is. The company has requested some independent consultation on the matter. As an independent consultant team, your tasks are

1. Perform an intrusion analysis on the provided network traffic log file to detect the infected system information, identify how the system got infected, what the infection was and the indicators of compromise with evidence.
2. Summarize the intrusion to understand what has happened, analyse it using Cyber kill chain and predict the next tactics using MITRE ATT&CK. Based on your investigation, suggest at least 1 Snort rule to detect similar attack(s) in the future with explanation.
3. More long term the company wants to know what techniques will be applied (for i.e. IDS, honeypots, SIEM), to what networks, the likelihood of finding the source of the issue, and how to detect/stop similar issues in the future. The long term plan should be explained to understand how similar incidents could be detected/ stopped.

Please note, **this is NOT a textbook exercise**. You are expected to undertake an experiment, document and analyse the results and produce a report detailing the process. You are also expected to devise a long term plan for detecting and responding to intruders. Whilst the lab session will provide a start to this experimentation, you will be required to complete additional work. ***It is critical in your report that you demonstrate application of knowledge rather than textbook-level factual knowledge.***

Submission Requirements:

- All students MUST enrol to their group in DLE. Without group enrolment, you will not be rewarded marks even if your name is in the report.
- 3000-word limit (the word count excludes the Coursework Title Page, the list of references, screenshots).
- Report submitted at as single Microsoft word file (not compressed, submitted as .docx) or pdf file to DLE. The submitted file must have **the title page** using the supplied Coursework Title Page on DLE **as the first page** and **the appendix with completed Generative AI Declaration as the last page.** The title page must show group number, members and their contribution. If any member does not contribute to the group work, please provide such

information in the Coursework Title Page. Members without any contribution to the group work will not be rewarded the marks. Members who do not enrol to their group in DLE will not be rewarded the marks either.

Acceptable level of generative AI tool use in this assessment element

The acceptable level of GenAI use for this element is detailed with the allowed uses listed below. This is split into three categories (**Solo Work** – work must be your own with no AI support, **Assisted Work** – some uses of AI tools allowed, **Partnered Work** – AI tools integral part of the work). If you have any questions, please contact the module leader.

Solo Work	You must not use generative AI tools.	☐
Assisted Work	You are permitted to use generative AI tools in an assistive role.	☒
Partnered Work	Generative AI tool use is required as an integral part of the assessment, but transparency is required.	☐

Table 2: Acceptable Level of generative AI use

Inline with the indicated acceptable level of AI use above, the following uses are acceptable:

- A1 – Idea Generation and Problem Exploration
- A2 – Planning and Structuring Reports or Projects
- A3 – Research Assistance
- A4 – Language Refinement

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.

Assessment Criteria:

The report MUST be structured as specified in the following table. Please be very careful and pay close attention to these instructions.

Content	Details	Marks
Coursework title page	Please use the provided Coursework Title Page on DLE and fill in the required information	
Section 1 – Methodology and results	Explaining how you perform the intrusion analysis to identify the infected system information (IP address, MAC address, hostname, user account name of the infected machine,...), presenting and explaining indicators of the infection with evidence, how the system got infected. Please provide the screenshots of the analysis using appropriate tool(s), inputs (the filters,…) and results as evidence of the analysis. There should be explanation of the inputs and outputs.	**40**

Section 2	Summarize the intrusion (e.g. what have happened, timeline) based on the analysis in section 2. Analyse the intrusion using cyber kill chain (e.g. explain which the intrusion phase maps with which stage of Cyber kill chain, if applicable) Predict the next tactics based on the previous analysis and using Mitre ATT&CK (e.g. what could be the next phases of attack, what tactics and techniques could the attackers use in these phases) Write at least 1 Snort rule to detect similar attacks in the future with explanation.	**30**
Section 3 – Long term plans for detecting and responding to intruders	Proposed long term plans with critical analysis (why have you chosen a particular action and what are its pros and cons, how can your solution protect the system and avoid similar incidents in the future). Linking it with the analysis in section 2 when applicable (e.g. what each particular action can detect/ prevent/ respond which attack phase).	**30**
References	List of references that you have used and cited in the report	
Appendix	Declaration of AI usage	

An illustration of the feedback template is presented in Table 2.

Threshold Criteria (these are indicative only):

Criteria	Fail (<40%)	Pass (40%+)	Merit (60%+)	Distinction (70%+)	Grade
Section 1– Methodology and results	Unclear methodology No meaningful results presented	A sound methodology applied to a reasonable set of data and tools. Results are presented in an appropriate fashion with an accompanying analysis and interpretation	A solid methodology, appropriately identified datasets and tools. Results are presented well with an accompanying critical analysis to provide a good level of depth and understanding to the incident.	A justified methodology, appropriately identified datasets and tools. Excellent presentation of results with an excellent critical analysis.	**/40**
Section 2	No meaningful summary of the intrusion No analysis of the intrusion No prediction using Mitre ATT&CK No Snort rule provided	Some meaningful summary of the intrusion Little analysis Some prediction with limited explanation Snort rule provided with little explanation	Clear and logical summary of the intrusion Clear analysis Clear prediction with good explanation Snort rule provided with clear explanation and linking to the investigation.	Clear and logical summary of the intrusion Excellent analysis Good prediction with very good explanation Snort rule provided with excellent explanation, linking to the investigation.	**/30**
Section 3 - Long term plans for detecting and responding to intruders	Little meaningful plan without any rationale. Few if any relevant references	Clear plan with some rationale. Some evidence of appropriate references	Detailed plan with proper rationale Good use of a number of relevant sources in an appropriate manner	Excellent plan with clear rationale An excellent set of appropriate references	**/30**
Feedback/Overall	*Additional feedback*				**/100**

Table 2: Feedback Template

Acceptable levels of AI use:

The table below provides the acceptable use categories for GenAI. Each assessment 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 the preparation of your submission.**	☐
Assisted Work	**Generative AI tools have been used to assist you to prepare your submission.** Please indicate below the general tasks for which you have used AI. Select all that apply.	☐
	A1 – Idea Generation and Problem Exploration Used to generate ideas, and to explore approaches to solving a problem, developing a design, or investigating a question. You must critically assess AI-generated suggestions and ensure your own intellectual contributions are central.	☐
	A2 – Planning and Structuring Reports or Projects Used to help outline the structure of reports, documentation and projects. The final structure and implementation must be your own work.	☐
	A3 – Research Assistance Used to locate and summarise relevant articles, technical documentation or online resources. The interpretation and integration of research into your submission remain your responsibility.	☐
	A4 – Language Refinement Used to check grammar, refine language or improve sentence structure in reports. AI should be used only to suggest improvements, and you should check the original meaning is preserved. You must ensure that code documentation accurately reflects the code and is correct.	☐
	A5 – Mathematical Calculations Used to suggest appropriate mathematical methods or to check solutions. AI should not be used to produce the mathematical workings and descriptions that you submit.	☐
	A6 – Solution Architecture and Design Used to help outline the architecture or structure of a technical solution, such as system components, class hierarchies, mathematical models, engineering designs or processes. The final design and structure must be your own.	☐
	A7 – Coding and Computational Assistance Used to generate example code, understand syntax, explore alternative implementation, use computational tools, or learn new coding or computational concepts. Any submitted code must be your own, and you must be able to explain it.	☐
	A8 – Review and Improvement of Technical Work Used to review code, calculations, models, designs, simulations, or other technical work; improve readability, structure or presentation; or help correct errors. AI should be used only to provide suggestions for improvement. You must ensure the output accurately reflects your knowledge.	☐
	A9 – Testing, Verification and Validation Support Used to create test cases, validate outputs or suggest edge cases for software testing, or guide verification and validation. You are responsible for test planning and interpreting results.	☐
	A10 – Data Analysis and Visualisation Used to suggest ways to analyse, present or visualise datasets. The analysis and interpretations that you present must be your own.	☐
	A11 – Other AI roles not listed above Please specify:	☐
Partnered Work	**P1 – Generative AI tool use forms an integral part of the assessment and is compliant with the assessment brief.**	☐

General Guidance

Extenuating Circumstances

There may be a time during this module where you experience a serious situation which has a significant impact on your ability to complete the assessments. 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-and-regulations/extenuating-circumstances

Plagiarism

All of your work must be of 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 persons' 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/essential-information/regulations/plagiarism

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

Turnitin (http://www.turnitinuk.com/) is an Internet-based 'originality checking tool' which 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 referencing 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://help.turnitin.com/new-links.htm?Highlight=guide

The university also had Draft Coach available on the online version of Microsoft Word. Draft Coach is a Turnitin plugin and provides instant feedback on how to address citation issues, grammar mistakes and matches with Turnitin's database.

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 which provides you with specific guidance about how to reference lots of different types of materials.