Cyber Incident Response Plan

Objectives and Evaluation

Project Plan

Name	Position	Email	Phone
Aidhan Mitsopoulos	Scrum Master	103598809@student.swin.edu.au	0428770628
Habib Mustawafi	Product Owner	102053200@student.swin.edu.au	0466368916
Numil Fernando	Development Team Member	103517163@student.swin.edu.au	0406164700
Thomas Davis	Development Team Member	103203475@student.swin.edu.au	0449619570

Huy Tran	Development Team Member	102559614@student.swin.edu.au	0403204649
Zahin Un Nafi	Development Team Member	103539510@student.swin.edu.au	0481834630

Table 1: Project Team

Document Change Control

Version	Date	Authors	Summary of Changes
1.10	13/3	Whole team	Creation
1.2	15/3	Zahin	Introduction
1.3	16/3	Zahin	Scope, Acceptance Criteria
1.4	23/3	Zahin	End of section 6
1.5	24/3	Aidhan	Clean up document
1.6	26/3	Whole team	Edited Deliverables, Scope and Critical Success Factors
1.7	28/3	Aidhan	Acceptance Criteria, Project Timeline, Assumptions and Budget

1.8	30/3	Whole team	Reworking of 1-4
1.9	31/3	Huy	Activities

Table 2: Document Change Control

Document Sign Off

Name	Position	Signature	Date
Aidhan Mitsopoulos	Scrum Master	Aidhan	02/04/23
Habib Mustawafi	Product Owner	Habib	02/04/23
Numil Fernando	Development Team Member	Numil	02/04/23
Thomas Davis	Development Team Member	Thomas	02/04/23
Huy Tran	Development Team Member	Huy	02/04/23
Zahin Un Nafi	Development Team Member	Zahin	02/04/23

Table 3: Document Sign Off

Client Sign off

Name	Position	Signature	Date
Dr. Rory Coulter			
Organisation			
Retrospect Labs			

Table 4: Client Sign Off

Table Of Contents

3. Establishment

3.1. Processes, Procedures and Standards

3.2. Project Environment

3.3. Project Team Skill Development Requirements

4. Deliverables, Activities and Capital Resources

4.1. Deliverables

4.2. Activities

4.3. Resources

5. Organisation and Structure

6. Risks

7. Schedule

7.1. Project Timeline

1. Introduction

The goal of this project is to create a Cyber Incident Response Plan and Evaluation system (CIRPAE) for Retrospect Labs. This document is meant for the project team, client, and other project stakeholders.

The project plan outlines the various activities that will be carried out in order to achieve the project objectives, such as collecting and analysing incident response plans, training a machine learning model with natural language processing techniques, and creating incident dialogue for validation purposes. It also provides details on the project scope, critical success factors, acceptance criteria, processes, procedures and standards, project team, risks, schedule, budget, and references.

By adhering to this project plan, the project team will be able to develop a complete CIRPAE system for Retrospect Labs in a timely and cost-effective manner. The plan will serve as a project roadmap, including essential activities and deliverables, as well as deadlines and resources needed. The plan will also help the client understand the project's scope, goals, and risks, and it will serve as a foundation for continuous project management and assessment.

1.1. Background

The Cyber Incident Response Plan and Evaluation (CIRPAE) project was initiated by Retrospect Labs to develop a comprehensive and effective incident response plan to cyber threats. The main goal of the project is to create an incident response strategy that Retrospect Labs and its clients can utilise to react to cyber threats swiftly and efficiently, safeguard vital assets, and limit the impact of events on company operations.

The rising frequency and severity of cyber attacks is driving the initiative. Cyber assaults have grown in sophistication, frequency, and severity, presenting a serious risk to enterprises of all kinds. This has made it critical for companies to be prepared to react to events promptly and efficiently. Retrospect Labs has undertaken this project to establish a thorough incident response strategy in response. The nature of the business domain necessitates a comprehensive and well-defined incident response strategy that addresses many sorts of cyber events, such as ransomware, phishing, and other types of cyber-attacks.

The project team, client, and other stakeholders are all key players in the CIRPAE project. The project team, which comprises a project supervisor, team leader, and key project members, is in charge of developing and implementing the CIRPAE system. Retrospect Labs, the project's client and sponsor is actively involved in project planning and implementation.

1.2. Key Project Personnel

The key personnel involved in this project are as follows:

- **Client:** Retrospect Labs
- **Project Supervisor:** Dr. Naveed Ali
- **Team Leader:** Aidhan Mitsopoulos
- **Key Project Members:**

1. Habib Mustafawi

2. Huy Tran

3. Numil Fernando

4. Thomas Davis

5. Zahin Un Nafi

1.2.1. Client

Retrospect Labs is a cybersecurity company founded in 2019 by former Australian Government Incident Responders, Jason Pang and Ryan Janosevic. CyRise, a venture-backed accelerator programme, accepted the startup in 2020. The objective of Retrospect Labs is to make cybersecurity accessible to all organisations by delivering creative, dependable, and cost-effective security solutions.

Retrospect Labs specialises in offering a platform for businesses to mimic different cyber threat situations, allowing them to educate their employees in proper cyber incident response. Companies may use Retrospect Labs' platform to run cybersecurity exercises and drills that simulate real-world scenarios and evaluate their capacity to react to a broad spectrum of cyber disasters. This enables businesses to uncover flaws in their cybersecurity measures and increase their overall preparation for cyber assaults.

1.2.2. Other Stakeholders

Project Supervisor:

The project supervisor is responsible for overseeing the project and ensuring that it is delivered on time, within budget, and to the satisfaction of the client. They will provide guidance and direction to the team leader and key project members, and will be monitoring progress while ensuring that all work is completed to a high standard.

Contact: Dr. Naveed Ali, email: nali1@swin.edu.au

Team Leader:

The team leader is responsible for managing the day-to-day activities of the project team and working closely with the team for developing the project. They will collaborate with the project supervisor and key project members to ensure that the project is delivered on time and within budget.

Contact: Aidhan Mitsopoulos, email: 103598809@student.swin.edu.au

Key Project Members:

The key project members are the individuals who will be responsible for developing the software along with the team leader and ensuring that it meets the requirements of the client.

Contact:

Habib Mustafawi, email: 102053200@student.swin.edu.au

Huy Tran, email: 102559614@student.swin.edu.au

Numil Fernando, email: 103517163@student.swin.edu.au

Thomas Davis, email: 103203475@student.swin.edu.au

Zahin Un Nafi, email: 103539510@student.swin.edu.au

1.2.3. Project Supervisor, Team Leader and Key Project Members

Position	Name
Project Supervisor	Dr. Naveed Ali
Scrum Master	Aidhan Mitsopoulos
Product Owner	Habib Mustafawi
Development Team Member	Huy Tran

Development Team Member	Numil Fernando
Development Team Member	Thomas Davis
Development Team Member	Zahin Un Nafi

Table 5: Team Roles

2. Terms of Reference

2.1. Objectives

The following will be the objectives for this project:

1. The GPT model is able to analyse a piece of dialogue and determine if the objective has been met by standards of a CIRP.

2. Determine validity of CIRP by comparing it against alternative CIRP's based off our human knowledge.

3. Model is capable of reading through a scenario and identifying possible threats within said instance.

4. The GPT model is to be able to comprehend security threats.

5. GPT Model should follow the criteria of C.I.A (Confidentiality, Integrity, Accessibility.)

6. Develop a user friendly interface so non experienced users can access it's functions.

2.2. Scope

2.2.1. In Scope

We have decided to build a software using an AI known as ChatGPT so that it is capable of being parsed XML or HTML files that contain CIRP playbooks through the use of advanced scripts provided through ChatGPT's developer mode library. The AI is expected to output identified objectives of each CIRP in paragraphs that summarize each recognized objective. Moreover, the responses are to follow the Cyber Security triad known as C.I.A when searching for each key objective. The prototype is expected to be fed a CIRP, once fed the user is then capable of asking said AI any questions relating to the response plans of any cyber threat, and providing a detailed response of it's findings. As to be expected the GUI for the prototype will be far less advanced than the final model, with it's only functions to respond to basic user imputed questions.

2.2.2. Out of Scope

However, the AI is not expected to provide steps on how to identify an attack or a potential threat nor will it be capable of form it's own CIRP from it's collected Objectives. In addition, the AI is an already constructed model found on the Internet and will only be trained to fit this projects needs. These topics are deemed out of scope and will not be a part of any model.

2.3. Critical Success Factors

•**People:** The use of regular communication held through meetings throughout each week ensures a consistent and unified focus on the task's by providing each other constructive criticism and streamlining the process of development.

•**Clarity:** Tasks to be performed must be clearly defined and planned thoroughly to prevent lackluster development of any future deliverables, ensuring the project remains on scope and does not deviate from expectation. Therefore, communication needs to be clear and articulate

•**Norms of Quality:** Deliverables and the expectations of the final product are to be conformed to, expectations of quality are to be maintained in order to provide worthy deliverables, prototypes and the final product.

•**Assessment of Risks:** Risks are ever present, thereby it is vital for them to be identified and planned for to mitigate potential risks to the development of the final AI model.

•**Realistic Calendar or Timeline:** As expected many of us have different lifestyles and activities, thereby the future agile Gantt chart is to be constructed around known holidays and or events that may impact our AI's development.

•**OpenAI Availability:** The OpenAI ChatGPT model should be readily available as we are not required to develop our own AI model, and will be using this as the skeleton of our software.

•**ChatGPT Developer mode funding:** The developer mode for ChatGPT is essential for the editing of the source code, as without it no customization to the training of the model will be possible.

•**Communication Software:** Softwares such as Discord are to be available and up and running 24/7 to ensure constant communication with each other and our supervisor.

•**GitHub Storage Space:** Github Free has a storage space of 2Gb's, thereby with a full storage, the constant updating of the AI's source code in tandem with added documents cannot be added to the repository. Therefore, free space within the repository is required for it's future changes.

•**Documentation Availability:** As this project will involve the ability to train an AI model to have knowledge of CIRP's, there must exist a number of widely available CIRP's that will be fed into the model.

2.4. Acceptance Criteria

1. The numerous of CIRP's fed into ChatGPT must have a high percentage (80%) of Objectives that properly follow the found Objectives identified by humans.

2. ChatGPT is to create or read instances from certain corporations's CIRP's and evaluate the effectiveness in the response of the scenario against their CIRP.

3. User Guide is to be provided so that anyone is capable of manipulating the trained software properly, such that our Client is fully capable of operating the mode.

4. The efficiency of the ChatGPT model must meet the 2 minute maximum time limit when analysing a possible complex CIRP playbook, to allow any future users to be able to feed it a document and receive a timely response.

5. The application is to be compatible with Windows 7-10/11 and MAC.

3. Establishment

3.1. Processes, Procedures and Standards

3.1.1. Processes

For this project, we will be adopting the Agile Project management and development methods to our construction of the project as it allows for iterative development and flexibility in responding to changing requirements. Moreover, we all so be using Scrum in tandem with Agile, using its methodologies to plot the timeline for our projects development as it encourages collaboration and continuous improvement.

In the case of Scrum, we have planned have 2, three week Sprints for the development of our project, with design and the AI's development in the first sprint with testing and it's deployment in the second sprint. In addition, it's deployment and evaluation will be conducted in it's following weeks.

3.1.2. Procedures

We will be using many different types of softwares to collaborate, store and plan the completion of the product:

These are:

- **Discord:** To be used to ensure collaboration for the team, in such we are capable of holding consistent daily meetings to synchronize our work log, provide instructions and communicate any information. Meetings are held 3-4 times a week with the average users for each being 4-6 people. This application is also used to provide links to other relevant software and to store the logs of each meeting.

- **GitHub:** To store each document, file and CIRP's we come across along with containing our future trained ChatGPT AI. GitHub will be used to manage source code and track changes. This will allow team members to work on different aspects of the project simultaneously while keeping the codebase in sync

- **Jira:** To document and plan our project timeline in accordance with Scrum whilst keeping in mind the ability to be Agile, we've decided to use the tool Jira. This will allow for a platform that the team is able to easily access and edit, allowing for continuous improvement.

To ensure efficient collaboration among team members and proper management of project resources, we will be using a version control system - specifically, Git - to manage source code and track changes. This will allow team members to work on different aspects of the project simultaneously while keeping the codebase in sync. Moreover, we shall be holding regular meetings 2-3 times per week to ensure our development cycle is being properly maintained and not deviating from our timeline of deliverables.

3.1.3. Standards

In addition to the versioning system, we will also adopt a user-centered design process to ensure that the cyber incident response plan objectives and evalua-

tion tool meets the needs of its users. This process will involve collecting feedback from stakeholders and end-users at various stages of the development process to inform design decisions and ensure the tool is user-friendly.

For this project, we will be using a pre-trained OpenAI or GPT model or train one from scratch to distill objectives from incident response plans and evaluate them via incident scribing. While we will be writing little code for this project, we will still adhere to established best practices when working with the AI model. This may include ensuring that the inputs are properly formatted, following any documentation or guidelines provided by the model's creators, and validating the outputs to ensure they are accurate and reliable. We will also ensure that any tools or scripts used to interface with the model are properly documented and version-controlled.

In regards to testing, each instance we feed a CIRP to the ChatGPT model, we expect the identified Objectives to meet a standard of 80% of our own human knowledge when reading CIRP playbook. Therefore, any instance where the AI does not meet our standards, it will be thoroughly altered andm re tested against the CIRP so it can potentially meet the 80% key objectives identified markup.

3.2. Project Environment

•**Workplaces:** The project team will primarily be working remotely, so each team member will need access to a computer with access to the internet.

•**Computers:** Each team member will need access to a computer that has an operating system such as Windows or Linux with Python installed. The basic system requirements to run and use. The minimum requirements are as follows:

- Operating Systems, 32/64-bit Operating Systems, Windows 7 or later, Ubuntu 16.04 or later, MAC OS X or later

- x86 64-bit CPU (Intel / AMD architecture). ARM CPUs are not supported. Minimum Intel Core-i3 processor required.

- 4 GB RAM.

- 5 GB free disk space.

•**User accounts:** The project team will need to create user accounts for OpenAI as the project will be based on OpenAI. The team members will also need to have a GitHub account for collaboratively coding on the software.

3.3. Project Team Skill Development Requirements

As the project will involve using a pre-trained open AI or GPT model or training one, team members will be required to gain knowledge on topics such as interacting with the OpenAI system, cybersecurity concepts and CIRP playbooks and Natural Language Processing (NLP) concepts.

Towards the later stages of the development of the project, the team will be required to have knowledge of coding using the language Python.

4. Deliverables, Activities and Capital Resources

4.1. Deliverables

The following will be delivered as part of this project:

- Project Plan
- Software Quality Assurance Plan
- Source Code
- System Requirements Specifications
- System Architecture Design and Research Report
- Detailed Design and Implementation Report
- Prototype
- User manual
- Final version of the software

4.2. Activities

•**Software Quality Assurance Plan:** To achieve this deliverable, we will need to prepare a list of reference documents that we have used for the project, assign management positions to the team, create documents regarding the project such as software documents and management documents. We will also need to set standards, practices, and conventions to ensure the quality of the software we are delivering, some of which would be Python PEP8 Coding standards, formatting standards and location/filename naming conventions. . There will also be the need to the project throughout its life-cycle and audits to ensure that processes are being adhered to. Once the software is being implemented, the team will also need to perform testing on the software. In the case of any issues throughout the project timeline, we will also need to report them and plan corrective actions. We will also include other key information such as risks, tools used in the project and methodology.

•**Source Code:** To further manipulate the AI into our expectations we will enter Developer mode for the ChatGPT model to alter any source code that may hinder it's training or add any code that is expected to improve the model.To display the source to any supervisor the source code will be provided through a compressed zip file to compress the large future Python package.

•**System Requirements Specification:** For this deliverable, we will be presenting this by giving a short description of the system and what it is about, from there we will identify and list what is required of the product, its features and on what criteria it will be accepted. We will also describe the function and requirements, whilst providing an overview on how the software will interact with other interfaces.

•**System Architecture Design and Research Report:** In this report, we will thoroughly research the problem that is presented to us and how we have designed a solution for it through our project. This will be closely linked to our System Requirements Specification document as we will be basing our architecture off the identified requirements. Presented within this report will also be a high level overview of our chosen system architecture, along with some other alternatives that we have explored. All relevant research that we will do to design and develop this solution will also be included in this report.

•**Detailed Design and Implementation Report:** Within this document, the design and methodology for how the project is to be implemented will be thoroughly planned. This document has 5 different key aspects to log our plotting of the implementation, these being an Introduction, System Architecture Overview, Detailed System Design and Implementation. This will follow our expected guidelines for our training of the AI and each aspect of this document will be filled in accordingly to our planned final product.

•Prototype Product Backlog:

No	Item	Dependencies	Business Value
F1	Integration of ChatGPT scripts to allow the parsing of HTML, XML and PDF data.		8
F2	CIRP can be successfully integrated into ChatGPT.	F1	10
F3	AI can interpret and identify objectives from CIRP	F2	10
F4	Formatting the AI to display identified objectives in dot points	F3	5
F5	Ensuring AI can follow for-	F3	7

	mat of C.I.A when analysing objectives		
F6	AI is to be tested against Human Knowledge of objectives in each CIRP	F3	8

Table 6: Product Backlog

•**User Manual:** This is to be filled with numerous instructions on how to operate the AI model to a basic extent, therefore guiding the user how to add a CIRP, then giving the user a basic prompt of questions he or she could ask the AI that would instigate proper responses. This method of how to use the ChatGPT model will be logged from our own personal usage of the AI.

•**Final Version:** The final version of the software will be created with a far more robust and trained version of the prototype's AI, having capabilities that include:

1. *GUI:* A far cleaner, more advanced and user friendly GUI to manipulate the ChatGPT model.

2. *Automation:* A model capable of being fed a large sum of numerous different CIRP's and having a successful answer rate when properly pointed to.

3. *PDF Printing:* The ability to print a PDF that contains all collected Objectives asked for by the User.

4.3. Resources

Links to resources which are relevant to the project that are available online such as: CISA Tabletop Exercises Packages, AWS Incident Response Playbooks, Threathunter Playbook and other cybersecurity exercises and CIRP playbooks have been provided by the client for training the AI model.

5. Organisation and Structure

Project Team:

- Project Supervisor

- Team Leader

- Team Members

Client:

- Project Sponsor

The organizational structure for this project will be a matrix structure, where each group is responsible for their respective deliverables and tasks. The project supervisor will be responsible for overseeing the project, ensuring that the project stays on track. The team leader and members will be responsible for communicating with the client, implementing the software, gathering, and analyzing relevant data. They will also be responsible for testing the software to ensure it meets the project requirements, creating the user and other project documentation. The client and the project supervisor will be responsible for providing feedback and ensuring that the project meets their requirements.

6. Risks

Rank	Name	Description	Likelihood of Occurrence	Severity	Mitigation Strategy	Contingency
1	Technical Risks	Potential technical difficulties with the software, hardware or infrastructure that could result in delays.	Medium	High	Regular system backups, maintenance checks and contingency plans in place to minimize downtime.	Implementation of a backup system and technical support team to handle any technical issues that may arise.
2	Resource Risks	The risk of not having adequate resources to complete the project on time and within budget.	High	Medium	Detailed planning of resource allocation and regular assessment of resource needs.	Reassessment of project scope and timelines, reallocation of resources or outsourcing to complete the project.
3	Communication Risks	The risk of miscommunication between team members and stakeholders which could result in misunder-	Medium	Medium	Regular project team meetings and progress reports, the establishment of clear lines of communication, and the	Clear documentation of project goals, timelines, and communication processes, and timely escalation of issues

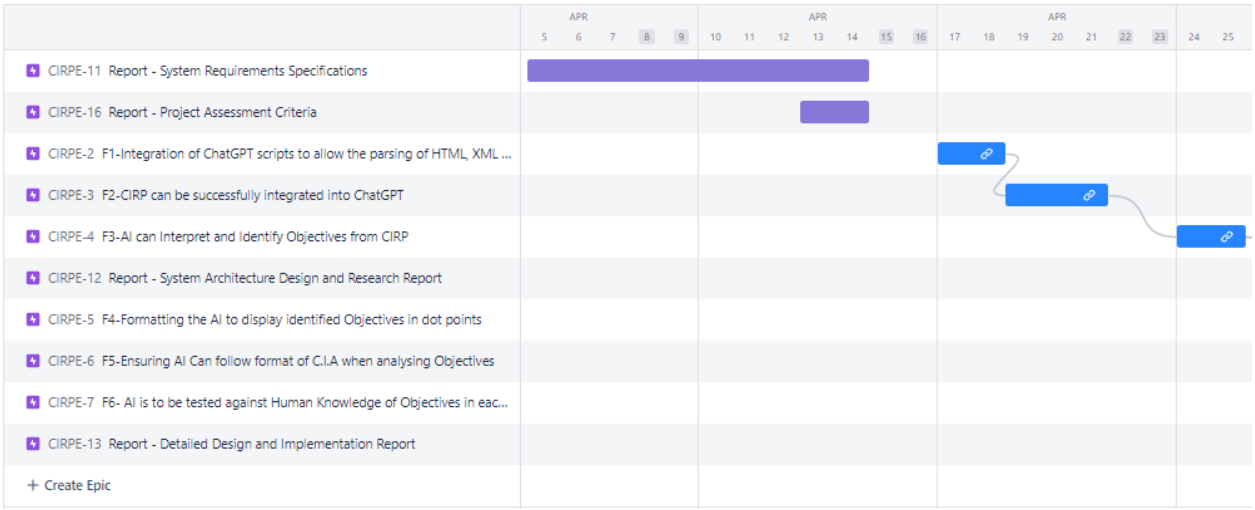
		standings or delays in project delivery.			use of collaboration tools such as project management software or chat platforms.	or concerns to management or other relevant parties.
4	Scope Creep Risks	The risk of scope creep, where additional requirements are added to the project without proper assessment of their impact on project timelines and budget.	High	Low	Detailed project requirements and scope documents, the establishment of a formal change management process, and regular review of project scope to identify any potential areas of scope creep.	Assessment of the impact of the scope change, and the implementation of a formal change management process to ensure the project remains on track.

Table 7: Assessment of Risks

7. Schedule

7.1. Project Timeline

Sprint 1

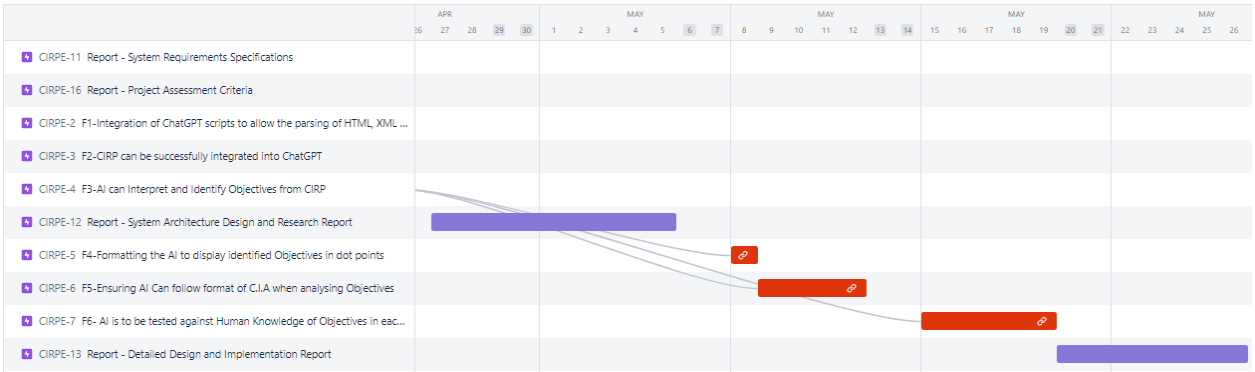


Item	Description	Date Start	Date End
Report	System Requirements Specifications	05 Apr	14 Apr
Report	Project Assessment Criteria	12 Apr	14 Apr

F1	Integration of ChatGPT scripts to allow the parsing of HTML, XML and PDF data.	17 Apr	18 Apr
F2	CIRP can be successfully integrated into ChatGPT	19 Apr	21 Apr
F3	AI can Interpret and Identify Objectives from CIRP	24 Apr	26 Apr
Report	System Architecture Design and Research Report	27 Apr	

Table 8: Sprint 1 Timeline

Sprint 2



Item	Description	Date Start	Date End
Report	System Architecture Design and Research Report		*05 May*
F4	Formatting the AI to display identified Objectives in dot points	08 May	08 May
F5	Ensuring AI Can follow format of C.I.A when analysing Objectives	09 May	12 May
F6	AI is to be tested against human knowledge of objectives in each CIRP	15 May	19 May
Report	Detailed Design and Implementation Report	*20 May*	*26 May*

Table 9: Sprint 2 Timeline

7.2. External Dependencies

Not Applicable

7.3. Assumptions

1. In the deliverables focused on testing, we have assumed that these will take a prolonged period of time due to past experiences of testing programs usually being prolonged due to errors in programs. Therefore, backlog items F6-F8 are deemed to take an average of 4 days to implement.

2. Moreover, the deliverables focused on integration are expected to take numerous hours as potential errors could arise while implementing backlog items F4,F3 and F1.

3. The assumption is made that the CIRP's that are found contain accurate information as that is what the GPT model will be basing its knowledge off.

4. In addition to this, we have also assumed that every team member, supervisor and client has a computer or device that meets the minimum requirements to run Python 3 as it will be required in project development.

8. Budget

8.1. Personnel Cost

Name	Rate per Hour
Aidhan Mitsopoulos (Product Owner)	50 AUD/hr
Habib Mustafawi (Scrum Master)	40 AUD/hr
Numil Fernando (Development Team Member)	40 AUD/hr
Huy Tran (Development Team Member)	40 AUD/hr
Thomas Davis (Development Team Member)	40 AUD/hr
Zahin Un Nafi (Development Team Member)	40 AUD/hr

Table 10: Project Personnel Cost

8.2. Time Estimated to Complete Each Task

Activity	Task	Estimated hours needed (hrs)	Total per activity (hrs)
F1	Integration of ChatGPT scripts to allow the parsing of HTML, XML and PDF data.		**20**
Subtask	Research and identify the best approach for integrating ChatGPT Open AI functions into the AI.	4	
Subtask	Implement the code to allow ChatGPT to parse XML or HTML files containing CIRP playbooks	6	
Subtask	Test the integration with sample CIRP playbooks to ensure it is working correctly	10	

F2	CIRP can be successfully integrated into ChatGPT		**30**
Subtask	Determine the format and structure of the CIRP files that will be accepted by ChatGPT	5	
Subtask	Modify the ChatGPT code to read and process the CIRP files	10	
Subtask	Validate that the CIRP files are correctly integrated into ChatGPT and are accessible to the user	15	
F3	AI can Interpret and Identify Objectives from CIRP		**30**
Subtask	Analyze the structure and content of CIRP files to identify the key objectives	5	
Subtask	Develop a machine learning algorithm to teach ChatGPT how	10	

	to recognize and interpret CIRP objectives		
Subtask	Test and refine the algorithm to ensure that it accurately identifies the key objectives in CIRP files	15	
F4	Formatting the AI to display identified Objectives in dot points		**10**
Subtask	Determine the format and style of the output for displaying the identified objectives	3	
Subtask	Modify the ChatGPT code to generate output in the desired format	4	
Subtask	Validate that the output is correct and properly formatted	3	

F5	Ensuring AI Can follow format of C.I.A when analysing Objectives		**40**
Subtask	Research and understand the C.I.A framework for cybersecurity	5	
Subtask	Develop a machine learning algorithm to teach ChatGPT how to follow the C.I.A framework when analyzing CIRP objectives	15	
Subtask	Test and refine the algorithm to ensure that it accurately follows the C.I.A framework when analyzing CIRP objectives	20	
F6	AI is to be tested against human knowledge of objectives in each CIRP		**50**
Subtask	Identify a set of CIRP playbooks with known objectives	2	

Subtask	Manually extract the key objectives from the CIRP playbooks	23	
Subtask	Test the AI against the set of CIRP playbooks and compare the output to the manually extracted objectives to ensure accuracy	25	

Table 11: Time Estimation for Tasks