**Cyber Incident Response Plan Objectives and Evaluation**

**Project Plan**

*List of your Names*:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **email** | **phone** |
| **Aidhan Mitsopoulos** |  | 103598809@student.swin.edu.au | 0428770628 |
| **Habib MUSTAFAWI** |  | 102053200@student.swin.edu.au | 0466368916 |
| **Numil Fernando** |  | 103517163@student.swin.edu.au | 0406164700 |
| **Thomas Davis** |  | 103203475@student.swin.edu.au | 0449619570 |
| **Huy Tran** |  | 102559614@student.swin.edu.au | 0403204649 |
| **Zahin Un Nafi** |  | 103539510@student.swin.edu.au | 0481834630 |

*SWE40001, Software Engineering Project A, Semester 1 2023*

|  |  |
| --- | --- |
|  |  |

**Document Change Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Authors** | **Summary of Changes** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*[Each time this document is revised, complete details of changes in Document Change Control table]*

# **Document Sign Off**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*[When document is finalised for submission, all team members must affix their signature in the Document Sign Off table]*

***[No-one should sign unless they have read the report and agree with it. ]***

# **Client Sign off**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |
| **Organisation** | | | |
|  | | | |

*[Client to sign off on the Project Plan to signify they agree with the plan]*

# **Contents**

**Introduction**

1.1. Background

1.2. Key Project Personnel

1.2.1. Client

1.2.2. Other Stake holders

1.2.3. Project Supervisor, Team Leader and Key Project Members

**2. Terms of Reference**

2.1. Objectives

2.2. Scope

2.3. Critical Success Factors

2.4. Acceptance Criteria

**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 Time Line

7.2. External Dependencies

7.3. Assumptions

**8. Budget**

**9. References**

**10. Tables Index**

# 

# 

# **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 CIRPOE 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 Mustawafi
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 Stake holders**

**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 Mustawafi, 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

**End-Users:**

The end-users of the software are a key stakeholder group, as the success of the project will depend on whether or not they find the software useful and easy to use. Their feedback and input will be important throughout the development process, and the team will work to incorporate their needs and preferences into the final product.

**Regulatory Bodies:**

Regulatory bodies that oversee the industry may have specific requirements that need to be met in order for the software to be used in the market. The team will need to ensure that the software meets all regulatory requirements and obtains any necessary certifications before it can be released.

# 

# **1.2.3.** **Project Supervisor, Team Leader and Key Project Members**

|  |  |
| --- | --- |
| **Position** | **Name** |
| Project Supervisor | Dr. Naveed Ali |
| Team Leader | Aidhan Mitsopoulos |
| Key Project Member | Habib Mustawafi |
| Key Project Member | Huy Tran |
| Key Project Member | Numil Fernando |
| Key Project Member | Thomas Davis |
| Key Project Member | Zahin Un Nafi |

# **2.** **Terms of Reference**

**2.1.** **Objectives**

Objectives

* The GPT model is able to receive a CIRP and determine the objective
* The GPT model is to be able to comprehend security threats
* The GPT model is able to analyse a piece of dialogue and determine if the objective has been met by standards of a CIRP.
* Determine validity of CIRP by comparing it against alternative CIRP’s

Objectives:

* The GPT model is able to analyse a piece of dialogue and determine if the objective has been met by standards of a CIRP.
* Determine validity of CIRP by comparing it against alternative CIRP’s based off our human knowledge.
* Model is capable of reading through a scenario and identifying possible threats within said instance.
* The GPT model is to be able to comprehend security threats.
* GPT Model should follow the criteria of C.I.A (Confidentiality, Integrity, Accessibility.)
* Develop a user friendly interface so non experienced users can access it’s functions.

# **2.2.** **Scope**

We have decided to train a ChatGPT model to be able to be fed sums of Cyber Incident Response Plans and Evaluate the Objectives from each document. The AI will not be able to provide steps on how to mitigate an attack or a potential threat, it will only be able to identify the objectives from each CIRP. The AI is also not expected to form a CIRP from the objectives it receives from it’s consumed CIRP’s. The AI will be fed data through the use of the Python Library known as Beautiful Soup from any HTML or XML file that contains a cyber incident response plan and output dotpoints of paragraphs or sentences that surmise the objectives it identified from each CIRP.

# **2.3.** **Critical Success Factors**

* The AI is to be able to surmise the Objectives pulled from each CIRP in clear concise sentences.
* The Objectives the AI identified have to match the Objectives we humans Identify and automate it through a much larger scale.
* The AI must follow the format of the Cyber Security Triad known as C.I.A to properly follow industry standards.
* The AI is to be able to read through a scenario and identify the flaws each objective of the scenario based off it’s knowledge.

# **2.4.** **Acceptance Criteria**

* The numerous of CIRP’s fed into ChatGPT must have a high percentage of Objectives that properly follow Cyber Security Objectives e.g C.I.A
* User Guide is to be provided so that he is capable of manipulating the trained software properly.

# **3.** **Establishment**

# **3.1.** **Processes, Procedures and Standards**

For this project, we will be adopting the Agile software development methodology as it allows for iterative development and flexibility in responding to changing requirements. The Agile approach also encourages collaboration and continuous improvement, which is essential for the success of this project.

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.

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 evaluation 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 pre-trained 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.

# **3.2.** **Project Environment**

Work places: The project team will primarily be working remotely, so each team member will need access to a suitable work environment.

Computers: Each team member will need access to a computer that meets the minimum system requirements for the tools and applications used in the project.

User accounts: The project team will need to create user accounts for any tools or services used in the project, such as the OpenAI or GPT model.

Stationary: The project team may require standard stationary supplies, such as pens, paper, and notebooks, for note-taking and other activities related to the project.

**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 conduct research and undergo training on this topic.

# **4.** **Deliverables, Activities and Capital Resources**

# **4.1.** **Deliverables**

The following deliverables will be produced as part of this project:

* Trained model: An open AI or GPT model will be trained to distill objectives from incident response plans and evaluate their effectiveness via incident scribing.
* Incident dialogue: A set of incident dialogues will be created to validate the trained model's performance.
* User documentation: User documentation will be provided to help users understand how to use the trained model and incident dialogue tool.
* Project presentation: A project presentation will be given to the project supervisor, team leader, and other stakeholders to demonstrate the project's outcomes and explain the methodology used.

Each of these deliverables will be completed by the end of the project and will be provided to the project supervisor, client and any other relevant stakeholders.

# **4.2.** **Activities**

The project will be executed using an agile development approach, with the following phases and associated activities:

**Phase 1: Planning**

* Define project scope and objectives
* Identify project stakeholders and their requirements
* Develop project schedule and budget
* Assign roles and responsibilities to team members
* Review and approve project plan

**Phase 2: Analysis and Design**

* Conduct research on existing incident response plans
* Identify key objectives and evaluation criteria
* Design and develop incident dialogue for model training
* Review and approve analysis and design documentation

**Phase 3: Development**

* Train the model using collected incident response plans
* Test and refine the model using incident dialogue
* Develop a system for incident scribing and evaluation

**Phase 4: Testing and Deployment**

* Test the model and incident scribing system
* Evaluate the effectiveness of the model and incident scribing system
* Deploy the model and incident scribing system

# **4.3.** **Resources**

Publicly available datasets that are relevant to the project for training the AI model has been provided by the client.

# **5.** **Organisation and Structure**

**Project Team:**

* Project Supervisor
* Team Leader
* Team Members

**Client:**

* Project Sponsor

**Other Stakeholders:**

* End-users
* Regulatory Bodies

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 | Data Privacy Risks | The risk of data breaches, which could lead to exposure of sensitive information | Low | High | Strict adherence to data privacy laws and regulations, implementation of encryption and other security measures to safeguard sensitive data. | Immediate notification of all affected parties, investigation of the cause of the breach, and the implementation of additional security measures to prevent further breaches. |
| 3 | 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. |
| 4 | Communication Risks | The risk of miscommunication between team members and stakeholders which could result in misunderstandings or delays in project delivery. | Medium | Medium | Regular project team meetings and progress reports, the establishment of clear lines of communication, and the use of collaboration tools such as project management software or chat platforms. | Clear documentation of project goals, timelines, and communication processes, and timely escalation of issues or concerns to management or other relevant parties. |
| 5 | 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. |

# **7.** **Schedule**

# **7.1.** **Project Time Line**

*[Given the tasks (group as activities) in Section 4.2, schedule each tasks using a Gantt chart or some other type of time line. You do not have to use Microsoft Project. Acceptable Gantt charts can be created using Excel or various graphics programs or can be hand-drawn]*

*[For each task, show the deadline, and who is allocated to each task (your team members). Often it is better to allocate two people to each task in case one becomes unavailable (e.g. breaks a leg)]*

# **7.2.** **External Dependencies**

*[Describe any inputs from external parties that are required to ensure that the schedule is met. These dependencies, if any, must also be indicated in the time line (Section 7.1) as a critical point]*

# **7.3.** **Assumptions**

*[Describe any assumptions that have been made in arriving at the schedule. These may be critical to the implementation of the software]*

# **8.** **Budget**

*[Summarise in a table the rate per hour for each of the team member. Look for an appropriate rate per work when doing such type of project. Using the role listed in Section 1.2.3, complete the table below]*

**Personnel Cost**

|  |  |
| --- | --- |
| **Name** | **Rate per Hour** |
|  |  |
|  |  |
|  |  |

Table 3 Personnel Cost

*[List all the tasks (grouped as activities) described in Section 4.2 in a table and estimate the number of hours needed to complete each task]*

**Time Estimated to Complete Each Task**

|  |  |  |  |
| --- | --- | --- | --- |
| **Activity** | **Task** | **Estimated hours needed (hrs)** | **Total per activity (hrs)** |
| ***1*** | *A* | *10* |  |
|  | *B* | *15* |  |
|  | *C* | *20* |  |
|  | *D* | *5* | *50* |
|  |  |  |  |
|  | *F* | *5* | *10* |
|  |  | Total |  |
|  |  |  |  |

Table 4 Task time estimate

*[As a guide in estimating the time consider the following:]*

*[Each team member should contribute equally, and time spent actually writing software should be about (200 hours x number of team members, ie, about 10 hours per week per member, excluding lectures) across the 2 semesters,*

*Total time allocation for each student should not exceed 10 hours per week,*

*The total hours per activity should be feasible within the schedule defined in Section 7.1]*

*[Note that the schedule in Section 7.1 includes slack time]*

# **9.** **References**

*[If you have used information from published sources, show where it came from. Use the Harvard system of citation. For instance, if it is from a website]*

***Your reference list entry must be in the form of***

**Author, Initial(s) Year, *Title of Document/Webpage/Website*, Organisation/Host, viewed Day Month Year, <URL>.**

example

Yates, J 2009, *Tax expenditures and housing*, Australian Housing and Urban Research Institute, viewed 12 November 2013, <http://www.ahuri.edu.au/publications/download/ahuri\_judith\_yates\_research\_paper>.

***Your in-text may be in the form of***

- **Direct quote**

"Most official estimates ..." (Yates 2009).

- **Paraphrase**

Yates (2009) looked at the equity implications of tax ...

***For more information on the Harvard style guide, refer to***

<http://www.swinburne.edu.au/lib/studyhelp/harvard_style.html>

# **10.Tables Index**

Table 1 Activities and Deliverables. 7

Table 2 Risks. 8

Table 3 Personnel Cost. 10

Table 4 Task time estimate. 10