Cyber Incident Response Plan Objectives and Evaluation

System Requirements Specification

Project Team - 02

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

SWE40001, Software Engineering Project A, Semester 1 2023

Document Change Control

Version	Date	Authors	Summary of Changes
1.10	8/4/23	Whole team	Creation
1.20	9/4/23	Whole team	Section 1 done
1.30	10/4/23	Whole team	Section 2 done
1.40	11/4/23	Whole team	Section 3 done
1.50	12/4/23	Whole team	Section 4 done
1.60	13/4/23	Whole team	Section 5 done

Document Sign Off

Name	Position	Signature	Date
Aidhan Mitsopoulos	Scrum Master	Aidhan	16/04/23
Habib Mustafawi	Product Owner	Habib	16/04/23
Numil Fernando	Development Team Member	Numil	16/04/23
Thomas Davis	Development Team Member	Thomas	16/04/23
Huy Tran	Development Team Member	Huy	16/04/23
Zahin Un Nafi	Development Team Member	Zahin	16/04/23

Client Sign off

Name	Position	Signature	Date
Dr. Rory Coulter			
Organisation			
Retrospect Labs			

1. Introduction

The software to be built upon is known as ChatGPT Open AI, with its main objectives to be capable of reading a Cyber Incident Response Plan (CIRP) playbook and retain the said documents main Key Objectives in handling specific Cyber Incidents so that it may describe and evaluate the effectiveness of their CIRP's.

1.1 Purpose

The purpose of this SRS document is to outline how the ChatGPT model is to be manipulated and trained to handle the proposed guidelines specified by our client. Therefore, demonstrating the requirements essential for the models final release. This document is relevant to any person wishing to gain an understanding of the essential requirements that the project team followed in the development of our CIRPA Artificial Intelligence. Moreover, this document explains the models architecture, purpose and it's requirements to be operated with explanations of our teams documentations and descriptions of our projects key aspects.

1.2 Scope

1.2.1 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.

1.2.2 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 project's needs. These topics are deemed out of scope and will not be a part of any model.

1.3 Definitions, Acronyms and Abbreviations

The following Definitions, Acronyms and Abbreviations will be used in the rest of this following document, these are:

CIRP = Cyber Incident and Response Plan

ChatGPT = ChatGPT open Ai model software.

CIRPP – Cyber Incident and Response Plan Playbook

C.I.A = The Cyber Security triad known as Confidentiality, Integrity and Availability.

2. Overall Description

The software being developed is a new and complete system, aimed at providing a solution for identifying objectives in Cyber Incident Response Plans (CIRP) using Artificial Intelligence (AI). The system will integrate ChatGPT scripts to allow the parsing of HTML, XML, and PDF data. The CIRP will be successfully integrated into ChatGPT, and the AI will be able to interpret and identify objectives from CIRP.

This system is not an upgrade or replacement of an existing product. It is a new system designed to meet the specific needs of identifying objectives in CIRP through the use of AI. The system is a complete product and is not a prototype or component of a larger system or library.

2.1. Product Features

The finalised model of our own ChatGPT model will have numerous significant features that will be far superior to the initial and basic Gradio model, these are:

- The ability to import CIRP playbooks.
- Objective Evaluation: The ability to evaluate CIRP's objectives and rate them accordingly against a success criteria that follows C.I.A.
- Capable of reading a dialogue and identifying if said scenario has met outlines of CIRP.
- Determine validity of a CIRP by comparing it against alternative but similar CIRP's.
- Framework of evaluation: Expectations of results

2.2. System Requirements

Hardware:

- 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.

Software:

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

2.3. Acceptance Criteria

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

2.4. Documentation

1. Project Plan
2. Software Quality Assurance Plan
3. System Requirements Specifications
4. System Architecture Design and Research Report
5. Detailed Design and Implementation Report
6. User manual

3. Functional Requirements

Description

The system being developed is being created to be fed cyber incident response plans and then provide the user with relevant information and advice. The output will vary depending on the prompt / input from the user, and it may provide tailor-made advice regarding an ongoing cyber incident or may be used to answer general questions.

Task and support

The task of the program is to provide advice on what to do in the case of a cyber attack, this will involve a user typing a prompt into the program which in return will provide a text response relating to the cyber threat. Using the information provided, the program will aid in identifying the type of attack, assessing the level of risk and then recommend the appropriate actions / response to mitigate the impact of the attack and possibly prevent it from occurring again.

The support would include the use of machine learning and natural language processing to accurately analyze information found within the provided pdf documents. The pdf documents being used within the program have been gathered from a range of different sources on the internet with each document providing unique and different advice whilst remaining logical and effective. The program's interface will have a clear output text box to make it simple and easy to understand.

Functions

- Users will be able to upload CIRP playbooks
- AI model uses OpenAI's model to interpret a user's input and generate relevant responses
- AI model will be able to follow Cyber Security triad (CIA)
- AI model will use provided cyber incident response plans as a knowledge base
- AI model will be able to analyse and identify CIRP objectives
- AI model can give a clear and concise response to questions asked by users relating to the response plans
- AI model will be able to provide a clear response with actions that should be taken in relation to a certain cyber incident

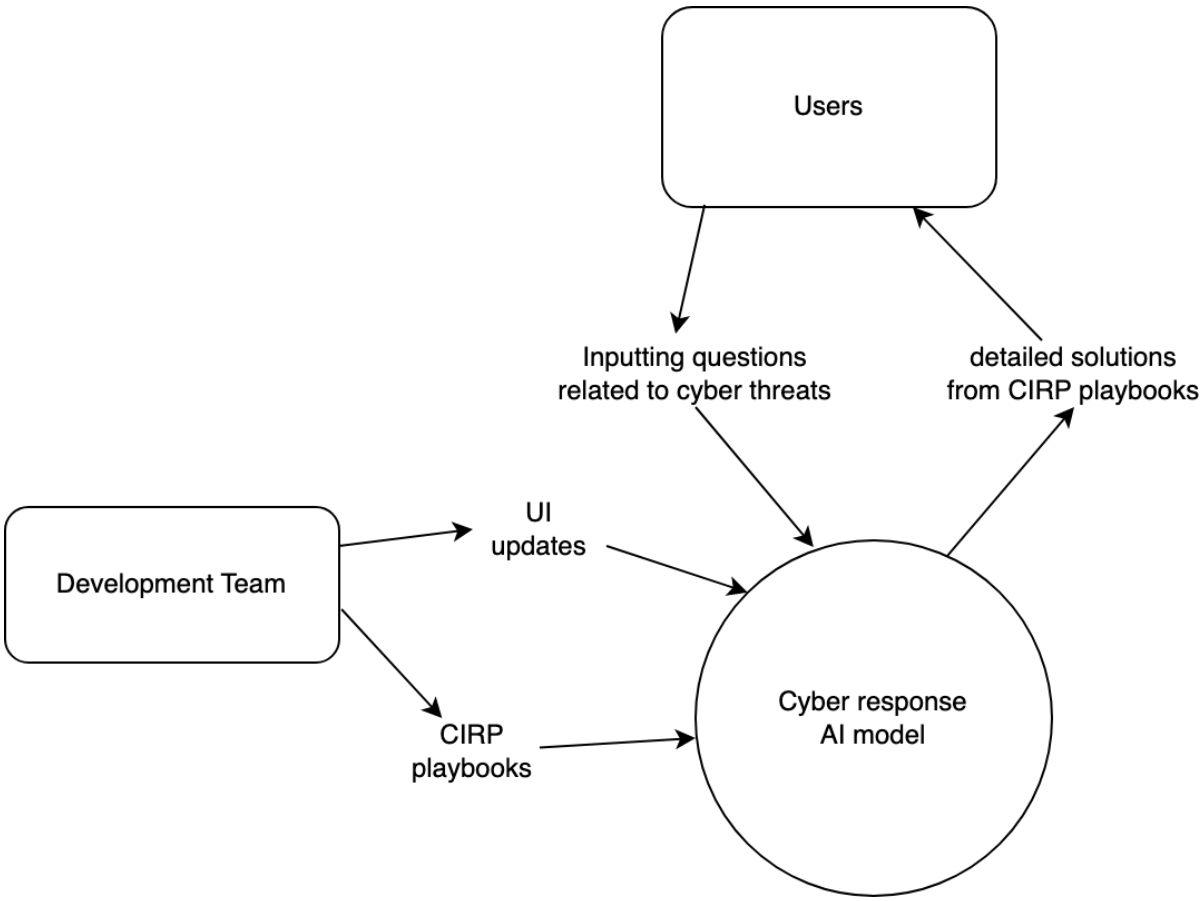
4. Non-Functional (Quality) Requirements

- **Efficiency:** The system should respond to user inputs and queries within a 10 second time frame. This can be verified by conducting load testing, stress testing, and measuring the system's response time under various usage scenarios.
- **Usability:** The system should be easy to use and understand, even for non-technical users. This can be verified through user acceptance testing, user feedback, and user satisfaction surveys. The users should be able to use the system after going through the user manual that will be provided.
- **Maintainability:** The system should be easy to maintain and update. This can be verified through maintainability testing, where the ease of updating and maintaining the system is tested by developers and system administrators
- **Functionality:** The system should provide accurate and reliable responses to user inputs and queries. This can be verified through accuracy testing, where the system's responses are compared against predefined responses for various inputs. This will be achieved if the responses provided meet at least a 95% accuracy. The remaining 5% of inaccuracy is expected as the model as the model can be further trained to increase the accuracy levels.
- **Availability:** The system should be available to use 98% of the time. The time where it is unavailable will be for patching and maintenance.
- **Portability:** The system will be available to use on multiple platforms. As there is no emphasis on the code involved in the system, the system will be able to be used on their desktops or laptops.

5. Interface Requirements

5.1. System in Context

The system that is being developed will have a thorough understanding of CIRP's. This system will then be used to educate the users on the purpose of CIRP's, the various cyber incidents that the user can face, their response to such incidents and how they can minimise these threats. Through this system, the client wants to explore the possibility of implementing AI models to play out cyber scenarios.



5.2. User Interfaces

The prototype will have a GUI that will consist of a textbox where the user will be able to input questions relating to the response plans and cyber attacks. There will be a “Submit” and “Clear” button under the textbox. Clicking “Submit” will issue a response from the AI Model in a separate textbox to the right of the screen. “Clear” will clear the user input textbox. Under the output textbox will also be a “Flag” button for malicious response by the AI Model.

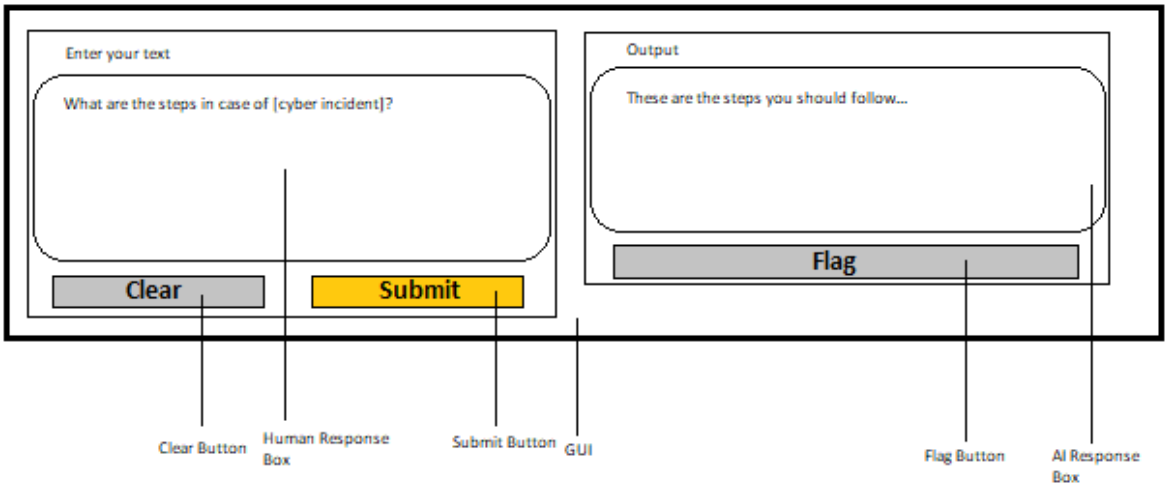


Figure: GUI Concept

5.3. Hardware Interfaces

The software has no hardware interface requirements.

5.4. Software Interfaces

The software does not interface with any other software applications.

5.5. Communication Interfaces

The software will use internet communication via HTTP/HTTPS protocol to communicate with external systems.