Software Requirements Specification

for

Kaiser Permanente Cybersecurity Project

Version 1.0 approved

Prepared by Danae O'Connor, Noah Warren, Bailey Hughes

University of Colorado Denver & Kaiser Permanente

Created: 9-8-2023

Table of Contents

Revision History

Name	Date	Reason For Changes	Version
Bailey Hughes	9/10/2023	First document write up	1.0.0

1. Introduction

1.1 Purpose

This product is made to be a visualization tool to translate detections of a cyber-attack into an understandable form. This will help in showing threats and also providing mitigation examples to these attacks.

1.2 Document Conventions

This document is structured in order from Introduction, Overall Description, External Interface Requirements, System Features, Other Nonfunctional Requirements, and Other Requirements. Each part has different labeled sub parts to break apart the bigger parts.

In addition to this structure for format – brackets "[...]" are items that are suggested but are yet to be determined, and parentheses "(...)" are primarily references to other parts of this document.

1.3 Intended Audience

Software Engineers – This document will show the other software engineers the intention of the software and the features of the software.

Kaiser Permanente Cybersecurity Team – This document will help the Kaiser Permanente Cybersecurity team get a better understanding of how the software works on the different features that the software provides.

Kaiser Permanente Directors – This document will be able to give a brief overview to the non-cybersecurity personnel of the basic objectives of this software and how it helps keep Kaiser Permanente safe from cyberattacks.

1.4 Product Scope

This software displays cards that display threat attack information from a cyberattack and plots it on an axis that is based either by the tactic's severity or the time the of the attacks on the x-axis and the attacks themselves are on the y-axis. This would allow a cyber-analyst user the ability to look at the different types of attacks in an organized manner to deal with the attacks more appropriately. This software will also print out a report that contains the graph information, intro, analysis, and a mitigation plan. This software will help the cybersecurity department at Kaiser Permanente to deal with cybersecurity threats more effectively.

1.5 References

References to other documents would go here as they are made or connected to the project in the future.

2. Overall Description

2.1 Product Perspective

This product is an additional component of a larger system. Kaiser Permanente has a detection system and a system or area to receive threat reports. This product is intended to interact with the detection software by pulling data from the detection system, labeling the attacks detected, and being able to export an overview of the attacks in an easily shareable format.

2.2 Product Functions

- Cards – Shows the cards of the different attacks and the information associated with those attacks.
- Tactic Priority View – Organizes the cards by attack tactic.
- Timestamp Priority View – Organizes the cards by the timestamp.
- Report Exportation – Allows the ability to export the report that also includes intro, analysis, and a mitigation plan.
- Visually Pleasant Design – Display data on the cyberattack in a clean manner.

2.3 User Classes and Characteristics

Current expected user is a cyber-analyst or a user with cybersecurity knowledge specifically around cyber-attacks. This software is meant to aid in analyzing a cyber-attack(s) through the tactics and techniques being used for the attack(s), so the user is currently expected to have some familiarity with cybersecurity, cyber-defense, or cyber-attacks.

2.4 Operating Environment

This will be an application that can run through any computer with the ability to use a web connected internet browser. It will use Splunk that is connected to the webpage. It will also use the information from the MITRE ATTC&K base for the card system.

2.5 Design and Implementation Constraints

The software will be running and displaying data through a webpage.
This software will be implemented with and therefore limited by the constraints of Splunk.

2.6 User Documentation

User document: (Document leading to user document when it is made)
MITRE ATT&CK Database: (Mitre website link will go here)

2.7 Assumptions and Dependencies

We plan to use The MITRE ATT&CK Database to obtain information about the various cyber-attack types and the different techniques for achieving each type of attack.

We also plan to use Splunk in order to visualize and display the attack data in an easy-to-understand card format, as well as exporting the data into a pdf report for easy sharing.

The user must have an internet connection with a computer able to run one of our supported browsers in order to be able to run the web page that contains the application.

3. External Interface Requirements

3.1 User Interfaces

All items on the user interface are still TBD since there needs to be more specification with the location of where the product will reside – which in turn will determine the aspects of capability.

[Current GUI is that there will be Cards (Feature 4.1) - which will display cyber-attack techniques in accordance with Mitre data and be categorized by tactics used – these cards will be layered in vertical columns with some kind of navigation to switch between units of time (Feature 4.3) or tactic category (Feature 4.2) on a timeline for either view. There will be a button to switch the view window from a Tactic Priority view (Feature 4.2) to a Timestamp Priority view (Feature 4.3), and an additional button to export a threat report of the given data. The cards are to be colored in a unique way to differentiate severity with the current idea being a light yellow for least severe all the way up to a bright red for the most severe, with an array of hues representing severity levels in between.]

3.2 Hardware Interfaces

This software is intended to be used with either a desktop or laptop platform. Given the product's web-based design, the software will work with both PC and Apple Mac hardware.

3.3 Software Interfaces

The software product will have the ability to run on any of the commonly used web browsers (Chrome, Safari, Edge, and Firefox).

[This could change if the product is a Splunk based item such as the Splunk Dashboards, meaning that it will be restricted to the browsers that can run Splunk. TBD.]

3.4 Communications Interfaces

[The way that this program will interface with any connecting software systems or databases are yet to be determined (TBD). Other items such as encryption or decryption for these communications are also TBD.]

4. System Features

4.1 System Feature 1 - Cards

4.1.1 Description and Priority

The function of the card feature is to display the incoming data from the Kaiser detection system on the main dashboard timeline in a card format when the application starts and begins collecting data. Displaying each cybersecurity attack technique as its own card will allow us to display some basic information about the attack, such as the technique name, a basic description of the way the technique works, and the type of tactic. This is to allow a cyber-analyst user to analyze incoming data.

Priority: High - 9

4.1.2 Stimulus/Response Sequences

When a new attack is detected by the Kaiser detection software, the information regarding the time of attack, name of the attack technique, and type of attack will be placed into a new card. The technique name will also be compared with MITRE's ATT&CK database to get some basic information about the technique, which will also be placed into the card. This card will then be displayed to the dashboard, as either a card in its corresponding tactic's deck, or based on its timestamp, depending on which Priority view the cyber-analyst user has selected (Features 4.2 and 4.3).

When a card is displayed to the screen, a user has the ability to click on the card, which will bring up all of the relevant information for that card. [Expand on information]

4.1.3 Functional Requirements

REQ-1: Each card will need to be populated using the data from the Kaiser detection software for each incoming attack.

REQ-2: Each card needs to contain the following information: The name of the technique, a timestamp for when the attack occurred, a basic description of what the technique entails, and the type of tactic the technique follows.

REQ-3: Each card will show a basic overview to the user when displaying the main dashboard. This overview will include the technique name and timestamp.

Once the user clicks on a card, the card will expand to display all the information present within the card.

REQ-4: If there is missing information for each attack technique coming from the Kaiser detection software, the card will still need to be generated, just without the missing information.

4.2 System Feature 2 – Tactic Priority View

4.2.1 Description and Priority

The function of this feature is to organize the display of technique cards when a cyber-analyst user begins using the application to analyze a cyber-attack. When the user chooses to display the cards using the Tactic based view, each card will be placed into a card deck with other cards that belong to the same cybersecurity tactic grouping. Each card deck will then be displayed on the dashboard timeline, allowing the user to click on it to expand the deck and view individual cards. This allows the cyber-analyst user to analyze a cyber-attack based on the tactics being used and the severity of the attack.

Priority – High - 8

4.2.2 Stimulus/Response Sequences

The main dashboard will feature a “toggle” to switch between the tactic’s view and the timestamp view.

When the user starts the application, the default view will be set to the tactic’s view, and the cards will be arranged into card decks based on the overall tactic of each technique.

If the application is instead in the timestamp view, when the user triggers the toggle, the cards will go from the arrangement of the timestamp view, back into the Tactics card decks.

When the user clicks on the deck corresponding to each Tactic, all of the technique cards present in that deck will be displayed and can then be expanded to display their information.

4.2.3 Functional Requirements

REQ-1: Each card must be placed into a deck corresponding to the overarching tactic that each technique belongs to.

REQ-2: Each card must display the technique name and timestamp when the deck is expanded to display all the cards in that deck.

REQ-3: Each deck must display the Tactic group that the techniques belong to, as well as the number of techniques currently in that deck.

REQ-4: Once each card is clicked on, the entirety of the card’s information must be displayed. Once a user is done viewing a specific card, the view must go back to showing the entire deck.

REQ-5: Once the user is done viewing a deck for a certain tactic, they need to be able to close the deck and return to the main dashboard view showing all the other tactics and their decks.

REQ-6: The tactic view will need a toggle to switch between the current view and the timestamp view. If the toggle is hit from the timestamp view, the cards will need to be arranged back into the deck’s based on their associated tactic.

4.3 System Feature 3 – Timestamp Priority View

4.3.1 Description and Priority

This feature is to represent the card feature (Feature 4.1) for the cyber-analyst user who is analyzing cyber-attack data from a detection system. When the user decides to use this priority view, it displays the technique cards and organizes the cards in a linear fashion in accordance with timestamps associated with the data for the cards. The timestamps are given by reported data from a Kaiser detection system. This allows the user the ability to see the cyber-attack information such as the tactics and techniques that are being used as the attack progresses along the timeline. [Expand on what]

Priority: High - 7

4.3.2 Stimulus/Response Sequences

There will be a button icon that will enable the swapping between this feature (the timestamp priority) and the tactic priority view on the main viewing screen. The user will click on the button, and it will swap from the Tactic Priority view, which is the default, to the Timestamp Priority view. The cards from the available data will then shift in accordance with the timestamps in increments (current estimate would be increments in seconds to increments in minutes – and potentially making it variable increment scale). When the Priority button is hit again it will swap back to the Tactic Priority view.

4.3.3 Functional Requirements

REQ-1: Need to base all information off the timestamps given by the data.
REQ-2: Need to display the data in the form of cards from the card feature (4.1).
REQ-3: Display available cards in given timestamp granularity, if there is a blank space where no cards exist in that timestamp needs to have a blank space shown.
REQ-4: A button that changes the view from Tactic Priority to Timestamp Priority. That same button should swap the Timestamp Priority to the Tactic Priority if the Timestamp Priority has already been selected.
REQ-5: A scrolling timeline that enables the view of the cards in a linear fashion – where the left side of the timeline is the earliest instance, while the right side is the latest instance.
[REQ-6: A button to swap the timeline making it so the latest instance is on the left and the earliest instance is on the right.]

4.4 System Feature 4 – Report Exportation

4.4.1 Description and Priority

This feature would allow the ability for the cyber analysis user of the software to export the data of the software to a PDF file. This file would contain the data from the system features 2 (Tactic Priority View) and 3 (Timestamp Priority Review), intro, analysis,

and mitigation plan. The ability to report the exportation would be a simple to find button on the webpage that says “Report Exportation”.

Priority: Medium - 6

4.4.2 Stimulus/Response Sequences

The cyber analysis user after generating a report within the webpage, would then press the button that says, “Report Exportation”. After the button is pressed it would then download a PDF file to the user’s computer of the report. The user could then open the file with their preferred PDF reader.

4.4.3 Functional Requirements

REQ-1: A button that says “Report Exportation” with the ability to click on the button.
REQ-2: The PDF report downloads to the cyber analysis user’s computer shortly after the button s
REQ-3: The ability to make the report into a PDF that is then downloaded to the cyber security analysis computer.

4.5 System Feature 5 – Visually Pleasant Design

4.5.1 Description and Priority

This feature allows the cyber-analyst user the ability to quickly understand the data on a cyber-attack by giving a report in the form of cards (Feature 4.1), a severity based on the tactics being used (Feature 4.2), or an analysis of frequency based on time (Feature 4.3).

The main viewing window should enable the swapping between Tactic Priority views of the cards and Timestamp Priority view. In addition, the cards displayed in both these views are colored to display severity levels based on the Tactic associated with the card data. [Current working theories are regarding saturation of reds or a variation of hues. For severe threats, the color should be a highly saturated red, while lower-level threats should be a yellow or light red. Exact method is TBD.]

In addition, in the Tactic Priority view and in the Timestamp Priority view there will be a horizontal scroll bar along the top and bottom edge of the view window that will enable the analyst user to view the data in the form of cards (4.1) in a linear fashion. The scroll bar only appears when there is enough data present to overflow the view window.

Priority: Medium - 5

4.5.2 Stimulus/Response Sequences

For the main viewing window, the default viewing of the card data should be in the Tactic Priority view.

There is a button that enables the swapping between Tactic Priority view and the Timestamp Priority view. When this button is clicked – the view will swap from Tactic Priority to Timestamp Priority, organizing the data by timestamps in accordance with feature 4.3.

By clicking the same button, it will swap from the Timestamp Priority view to the Tactic Priority view in accordance with feature 4.2.

4.5.3 Functional Requirements

REQ-1: Need to display the data in the form of cards.

REQ-2: Need to display the cards in both the Tactic Priority view and the Timestamp priority view.

REQ-3: Need a horizontal scroll bar on the top and bottom edge of the viewing window for viewing ease for when there is an overflow of data for the viewing window.

REQ-4: Need a button that switches the Tactic Priority view to the Timestamp Priority view, and that same button should switch from the Timestamp view to the Tactic Priority view.

REQ-4: Need a button that allows the user to shift the current Priority view's data in the following ways:

Tactic Priority:

Shift data from the least severe threat on the left side of the view and most severe threat on the right side of the view into the most severe threat on the left side of the view and least severe threat on the right side of the view.

Timestamp Priority:

Shift data from earliest instance threat on the left side of the view and latest instance threat on the right side of the view into the latest instance on the left side of the view and the earliest instance on the right side of the view.

REQ-5: Need a button that allows the analyst user to export a report in the report feature format (Feature 4.4).

5. Other Nonfunctional Requirements

5.1 Performance Requirements

[Needs to be able to handle years' worth of cyber-attack detection data. Exact implementation and processes constraints are TBD. The software must be able to run on most modern browsers without any issues.]

5.2 Safety Requirements

[More expectations regarding specific safety requirements are To Be Determined.]

5.3 Security Requirements

This software should only be used by authorized personnel, and safety precautions should be in place to make sure that only authorized personnel are allowed to use this software. A login system would be introduced to make it harder for unauthorized personnel to access this software.

This software could contain information important to the cybersecurity of Kaiser Permanente, and extra steps should be taken to safeguard this data.

5.4 Software Quality Attributes

[To be determined – current software attributes are visually pleasant design which is interpreted as having minimal buttons (less than 10), having accessible information (less that 10 clicks or actions to get to any given feature), and having a design that has good coloration for both information display and ascetics – such as Cards (Feature 4.1) having a hue range from yellow to red depending on severity, as well as having a background that allows for the information to be seen.]

5.5 Business Rules

This would be up to the Kaiser Permanente client. We would need to ask which individuals have authority to perform specific actions within the software.

[Please refer to the client to fill out this part as other information is TBD.]

6. Other Requirements

[Other requirements such as database size is TBD.]

Appendix A: Glossary

Cards – a reference to system feature 4.1 which is to display data of a cyber-attack in accordance with technique.

Appendix B: Analysis Models

No models are currently developed or shown.

Appendix C: To Be Determined List

Need to further develop the user interface – what it is intended to look like, where it will reside (Splunk or some other webpage) and the navigations that are wanted or desired.

Need to further develop the software interface primarily if the product is to be held on the Splunk platform or some other webpage.

Need to define the communication interface, how the product will communicate to other databases and how frequently as well as any conventions or necessities to talk to intended external resources.

Need to further develop the colorations of Cards (Feature 4.1) for sorting the techniques by Tactic – primarily the color since there are 14 tactic types at the time of writing (9/14/2023), and 14 shades of red could cause multiple issues.

Need to further develop the Performance requirements.

Need further description of Safety requirements.

Need further information on the Software Quality Attributes such as ease of navigation or what visually pleasant design means.

Need to know if there are Business Rules that may influence how this product is intended to function.

The software could recommend mitigation tactics that are not an appropriate way to deal with the problem, potentially causing a cybersecurity threat to get worse. It is important to include a disclaimer that mitigation tactics may not be the best possible action for a given situation.

Need to know if there are Other Requirements such as database size.