Requirements Document

for

Kaiser Permanente Cybersecurity Project

Version 1.0 approved

Prepared by Bailey Hughes, Danae O’Connor, and Noah Warren

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
Danae O’Connor	9/19/2023	Rewrite of the document – clarifying details and systems	1.0.1

1. Introduction

1.1 Purpose

This product is made to be a visualization tool to visually represent an on-going cyber-attack via detections and display it in an understandable form that contains the severity of the attack, the type of attack, and a description of the attack being used. This will help in showing the types of cyber-attacks that are used against Kaiser Permanente systems.

1.2 Document Conventions

This document is structured in order of: 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 other software engineers the intention of the software and its provided features.

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

Kaiser Permanente Directors – This document will 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 (Feature 4.1), which act like a deck of cards or a stack of notecards, 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 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 various types of cyber-attacks in an organized manner to deal with the attacks more appropriately. This software will also print out a report that contains an introduction, graph information, and an analysis of the make-up of the cyber-attacks. 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 one component of a larger system. Kaiser Permanente has a detection system that places the data from the detection into their specific Splunk database. This product is intended to interact with the data from the detection software by extracting the cyber-attack Tactic, Technique, and time of the cyber-attack and technique ID from the analyzed attack. Using this data, the product will display the information in a card format (Feature 4.1) and organize it in a linear fashion along a timeline by either the priority of the tactic – going from least severe attacks to the most severe – or organize it chronologically with the timestamps. From this collection of data, there will be an ability to export an overview of the attacks in a PDF file for a threat report which will contain the following information: the visual form of the analysis (the visual view) and a list of the viewed items organized by the view (by tactic or by timestamp) selected at the time of the export.

2.2 Product Functions

- Cards – Shows the card feature (Feature 4.1) which displays cyber-attack Tactics, Technique, attack description, and time of the attack on the card. [This display only happens when specifically selected.] Each card is created by the techniques used and classified by the tactic the technique belongs to.
- Tactic Priority View – Organizes the cards by attack tactic.
- Timestamp Priority View – Organizes the cards by the timestamp associated with the detected attack.
- Report Exportation – Allows the ability to export the report that also includes an introduction, an analysis that contains the visualization and the list of the items in the visualization organized by the view selected at the time of the export, [and a mitigation plan].

2.3 User Classes and Characteristics

The 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 visually representing the tactics and techniques being used for the attack(s), so the user is expected to have some familiarity with cybersecurity, cyber-defense, or cyber-attacks.

2.4 Operating Environment

This will be a Splunk application to be published within the "splunkbase" application hub. This will require the cyber-analyst user to have a Splunk account and the latest version of Splunk Enterprise to use the application. The information that will populate the cards (see Feature 4.1) will come from the Kaiser Threat Detection System.

2.5 Design and Implementation Constraints

The software will be implemented as a Splunk Application. It will gather data from the Kaiser Detection System, which will determine how quickly the application receives the attack data.

2.6 User Documentation

User document: (Document leading to user document when it is made)
MITRE ATT&CK Database: https://attack.mitre.org/datasources/
Splunk will be used as the primary database/area for data to reside that will contain detection data [and MITRE ATT&CK data]. Splunk will also be the platform for the visualization tool this product is created for.

2.7 Assumptions and Dependencies

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

Splunk will be used to visualize and display cyber-attack data in the card format (Feature 4.1), as a visualization, and exporting the data into a PDF report for reporting the attack.

The user must have an internet connection with a computer able to run one of our supported browsers (see section 3.3) 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 to be determined 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.

[The user interface is that there will be Cards (Feature 4.1) - which will display cyber-attack techniques - which is categorized by MITRE ATT&CK data – and be categorized by tactics used. These cards will be layered in some way with navigation controls to switch between the views of units of time (Feature 4.3) or tactic classification (Feature 4.2) on a timeline/scrolling-view for either option. There will be a way to switch the view window/area from a Tactic Priority view (Feature 4.2) to a Timestamp Priority view (Feature 4.3), and an additional way to export a threat report of the given data. The cards are to be colored in a unique way to differentiate severity with light yellow for least severe cyber-attacks all the way up to a bright red for the most severe cyber-attacks scaling with several hues for the other attacks.]

{Add color chart here for all 14 tactic categories}

3.2 Hardware Interfaces

This software is intended to be used with either a desktop or laptop platform. As a Splunk application, the software will work on personal computers with Windows, Apple Mac, and Linux/Unix hardware as long as it aligns with the Splunk requirements put forth in this site: https://docs.splunk.com/Documentation/Splunk/9.1.1/Installation/Systemrequirements

3.3 Software Interfaces

The software will be developed as a Splunk application. As such, it will require the cyber-analyst user to have an up-to-date installation of Splunk Enterprise. The primary method to interface with the application will be in Splunk Web, which is Splunk Enterprise's Graphical User Interface. This will require the cyber-analyst to have the latest version of either Chrome, Firefox, Safari, or Edge.

3.4 Communications Interfaces

The communication interface between the product and the data is that the cyber-attack detection data must be uploaded to Splunk which contain the following fields: Tactic, tactic id, technique, time, and description. [The tactic determines the class of cyber-attack and its severity, the tactic id is the MITRE ATT&CK ID that identifies the cyber-attack, the timestamp is the time of the attack/or the time that Splunk indexes the attack, and the description contains the description of the attack's technique \]
There is no encryption or decryption processes due to this application being integrated into a secure interface and secure system with no outward interactions via the internet or other unsecure channels.

4. System Features

4.1 System Feature 1 - Cards

4.1.1 Description

The function of the card feature is to display the incoming data from the Kaiser detection system that has been placed into a Splunk database on the products primarily visualization timeline window in a card format. The card displays each cybersecurity attack technique as its own card will allow us to display some information about the attack including the technique name, a technique id, the tactic the technique belongs to, a brief description of the way the technique works, and the time that the cyber-attack took place. This is to allow a cyber-analyst user to analyze the incoming data from a cyber-attack.

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 it which will bring up all of the relevant information for that card.

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

The function of this feature is to organize the display of technique cards (Feature 4.1) 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.

4.2.2 Stimulus/Response Sequences

The main dashboard will feature a "toggle" to switch between the tactic's view and the timestamp view. The user – the cyber-analyst – will interact with the toggle which will swap from the Tactic view (Feature 4.2 - this feature) which is the default view, to the Timestamp view (Feature 4.3).

When the user begins using this product, the default view will be set to the tactic's view, and the cards (Feature 4.1) will be arranged into card decks based on the overall tactic category of each technique and placed onto a timeline.

If the application is instead in the timestamp view (Feature 4.3), when the user triggers the toggle, the cards will go from the arrangement of the timestamp view (Feature 4.2 - this feature), back into the Tactics card decks.

When this view is selected and the user clicks on a deck corresponding to a Tactic, all of the technique cards present in that deck will be displayed. A singular card can be clicked which will cause the card to expand and display that card's information: technique name, tactic type, description of the attack, and the time the attack took place.

4.2.3 Functional Requirements

REQ-1: Each card must be placed into a deck corresponding to the overarching tactic category 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 a card is clicked on, the entirety of the card's information must be displayed: technique, technique id, tactic, timestamp, and description. Once a user is done viewing a specific card, the view must go back to showing the entire deck [currently clicking away from the currently viewed card or selecting another card].
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

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 which has been placed into the Splunk database/data collection area where this application resides. When the user decides to use this Timestamp Priority view, it displays the technique cards and organizes the cards chronologically along a timeline by the timestamps associated with the data in the cards for the time of the cyber-attack. The timestamps are given by reported data from a Kaiser detection system placed in the Splunk data area associated to the cyber-attack information, including tactic and technique of the attack. This allows the user the ability to see the cyber-attack's information such as the attack tactics and techniques that are being used in a cyber-attack as the attack progresses.

4.3.2 Stimulus/Response Sequences

On the main viewing window, there will be a display of the cards (Feature 4.1) that will be aligned in a chronological order in accordance with the timestamps of the given data.

There will be a toggle that will enable the swapping of views between this feature (the timestamp priority) and the Tactic Priority view (Feature 4.2) on the main viewing screen. The user will interact with the toggle, and it will swap from the Tactic Priority view, which is the default, to the Timestamp Priority view (Feature 4.3 - this feature). 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 associated with the cyber-attacks from the data collected by the detection system and placed into Splunk.
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 time-view granularity. [If there is a blank space where no cards exist in that timestamp needs to have a blank space shown.]
REQ-4: A toggle that changes the view from Tactic Priority to Timestamp Priority. That same toggle swaps 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 and chronological fashion – where the left side of the timeline is the earliest instance of a cyber-attack, while the right side is the most recent instance of a cyber attack.

4.4 System Feature 4 – Report Exportation

4.4.1 Description

This feature would allow the ability for the cyber-analyst user of the software to export the software's data to a PDF file. This file contains visualization of the data from the Tactic Priority View (Feature 4.2) and Timestamp Priority View (Feature 4.3), an introduction, analysis, and mitigation plan. There will be an ability to export the report.

4.4.2 Stimulus/Response Sequences

The cyber-analyst user interacts with an item to generate the report. The report is generated from the view the user is on at the time of the interaction. The generated report contains: Introduction, the visualization seen by the user, and a list of the items in the visualization.
After generating the report, the user will interact with a confirm button. After the button is pressed it would then download a PDF file of the report to the user's computer. The user could then open the file with their preferred PDF reader as this is not a functionality of this product.

4.4.3 Functional Requirements

REQ-1: An interaction item that allows for a report to be generated.
REQ-2: An interaction to confirm the report and print it as a PDF to the user's system.

REQ-3: The ability to use the visualization tool’s data and print that data into a report.

4.5 System Feature 5 – Visually Pleasant Design

4.5.1 Description

This feature allows the cyber-analyst user the ability to understand the data on a cyber-attack by giving a report in the form of cards (Feature 4.1), a severity-based view of the cyber-attacks by the tactics and techniques being used (Feature 4.2), or an analysis 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 cyber-attacks, the color should be a highly saturated red, while lower-level cyber-attacks should be a yellow.]

In addition, in the Tactic Priority view (Feature 4.2) and in the Timestamp Priority view (Feature 4.3) the user will have the ability to navigate the view window to view data that cannot fit on the window or see the more of the data along a timeline. This will enable the cyber-analyst user to view the data in the form of cards (4.1) in a linear fashion depending on whether the user wants to view the data in terms of tactic categories or chronological progression.

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 (Feature 4.2).

There is a toggle that enables the swapping between Tactic Priority view (Feature 4.2) and the Timestamp Priority view (Feature 4.3). When this toggle is triggered – the view will swap from Tactic Priority (Feature 4.2) to Timestamp Priority (Feature 4.3), organizing the data by timestamps in accordance with feature 4.3.

By triggering the same toggle, it will swap from the Timestamp Priority view (Feature 4.3) to the Tactic Priority view (Feature 4.2) and organize the data by tactic category in accordance with feature 4.2.

4.5.3 Functional Requirements

REQ-1: Need to display the data in the form of cards (Feature 4.1) which displays tactic category, technique, description of the technique, and the timestamp of the cyber-attack.

REQ-2: Need to display the cards in both the Tactic Priority view (Feature 4.2) and the Timestamp priority view (Feature 4.3).

REQ-3: Need a way to navigate for when there is an overflow of data for the viewing window.

REQ-4: Need a toggle that switches the Tactic Priority view (Feature 4.2) to the Timestamp Priority view (Feature 4.3), and that same toggle should switch from the Timestamp view to the Tactic Priority view.

REQ-5: Need a way to allow the cyber-analyst user the ability to export a report in the report feature format given in 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 to be determined and are restricted by Splunk's capabilities, as well as any restrictions the detection system may present. 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. Splunk Enterprise includes a login system 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 Kaiser Permanente. They will determine which individuals have authority to perform specific actions within the software.

Other Requirements

[Other requirements such as database size is to be determined.]

Appendix A: Glossary

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

Tactic – The most abstract description of the type of cyber-attack. Each technique belongs to one or more tactics which define their goals and objectives.

Tactic View – A reference to System Feature 4.2, the Tactic Priority View, in which the cards are displayed in groups corresponding to their associated tactic.

Timestamp – The time at which each cyber-attack occurred.

Timeline – Refers to the graphical depiction of the cards according to when the cyber-attack(s) occurred.

Timestamp View – A reference to System Feature 4.3, The Timestamp Priority View, in which the cards are displayed along a timeline according to when the attack was detected.

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.