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

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
Danae O’Connor	1/19/2024	Initial Revision for updated information	1.1
Noah Warren	1/23/2024	Completing Revision for updated information	1.1
Noah Warren	1/24/2024	Format Correction and Information Clarity.	1.2
Danae O’Connor	1/25/2024	Format Correction and Infromation Clarity.	1.2
Danae O’Connor	1/26/2024	Corrections to Format & Information Clarity	1.2
Noah Warren	1/28/2024	Final confirmation of edits and grammar check	1.2
Noah Warren	5/1/2024	Final annotations of the functions of the product.	1.3

1. Introduction

1.1 Purpose

This product is made to be a visualization tool for the Splunk Enterprise system to visually represent an on-going, or previous, cyber-attack or attacks 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. By using information about the attack, including the type of tactic severity and techniques used – with data obtained from a different system and classified by the industry standard MITRE ATT&CK – this application will be able to translate the data into either a Tactic View form where in the cyber-attacks are represented by the various tactic categories being used or a Timeline View form where the cyber-attacks are displayed by the times at which they occurred. This will aid 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 Appendices. Each part has different labeled sub-parts to break apart the bigger parts. In addition to the overall formatting structure, parentheses "(...)", are primarily used to indicate references to other parts of this document or an abbreviation of a term that will be used. There are multiple conventions and terms that are used throughout this document, and it is recommended that all readers read through Appendix A: Glossary before reading through sections 2 through 5.

1.3 Intended Audience

- Software Engineers
  - This document is written to show other software engineers the intentions of the software and the features it provides.

- Kaiser Permanente Cybersecurity Team
  - This document is intended to help the Kaiser Permanente Cybersecurity team understand how the software works and describe its features.

- Kaiser Permanente Directors or other non-security members
  - 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), that display cyber-threat information from a cyberattack and plots it on a horizontal x-axis that is based either by the tactic's severity or the time of the attacks and the attacks themselves are on the vertical y-axis in columns or "stacks". This would allow a cyber-analyst user the ability to look at the various types of cyber-attacks utilized against a system in an organized manner. This software was initially intended to integrate with Splunk Enterprise's system to print out a report containing the visualization of the graph and the graph information but was removed by the client in the fall of 2023 and was given up in persuit of other functionalities of the product.

1.5 References

The classification references in this document are attributed to the MITRE ATT&CK database of cyber-attacks. https://attack.mitre.org/datasources/

This product is designed as a visualization tool for Splunk Enterprise, a product of SPLUNK. https://www.splunk.com/

2. Overall Description

2.1 Product Perspective

This product is one component of a larger system. Kaiser Permanente, our client, has a threat detection system and a system that places the data from that detection system into their specific Splunk Enterprise database. This product is intended for those familiar with cyber-security or cyber-attacks to use this product to aid their analysis of cyber-attacks and has access to such data.

This product is intended to interact with the data from the detection software by extracting the cyber-attacks' Tactic category name, Technique name and ID, a description of the attack, the time the attack took place, and the title associated with the attack. By using this data, the product will display the information in a "card" format (see Feature 4.1) and organize it in a linear fashion along a timeline by either the priority of the represented tactics – sorting from the least severe category of attacks to the most severe category – or by organizing it chronologically based on the timestamps of each attack. From this data collection, the cyber-analyst user can export an overview of the cyber-attacks with Splunk Enterprise's printing tool. The exported report contains the following information: the visual form of the data (either the tactic or timeline view of the data, depending on what view is on screen when the report is generated) and a list of the viewed items organized by either the tactic or timestamps (depending on which is present on screen at the time of the export).

2.2 Product Functions

- Cards – Shows the card feature (Feature 4.1) which displays cyber-attack tactics, techniques, attack descriptions, the title of each attack, and the time of each attack on the card. There is also a truncated version for each card which displays only the technique and timestamp. This version is the default, and the full card is only displayed when the user hovers their mouse over the truncated card on the visualization.
- Tactic Priority View – Organizes the cards by attack tactic. The tactic of the cyber-attack is categorized by the industry standard MITRE ATT&CK database, and each technique is sorted into 1 of the 14 different tactic categories classified by this database. This view sorts the attacks by the severity of the tactics represented in the given cyber-attacks.
- Timeline Priority View – Organizes the cards by the timestamp associated with the detected attack. The cards are placed chronologically with the most recent cyber-attack in the data set

being placed on the far right of the visualization with the earliest cyber-attack in the data set being placed on the far left of the visualization.

- Report Export – Allows the ability to export the report that contains the visualization and the list of the items in the visualization organized into the view selected at the time of the export.

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 cyber-attack(s) as well as the times the attack(s) took place, 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 Enterprise application to be published within the “splunkbase” application hub. This will require the cyber-analyst user to have a Splunk Enterprise account and version 9.1.1 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 Enterprise Application and works as a visualization tool. The data used in the product is gathered from a separate system and put into the Splunk Enterprise data-system where the application can access it. As such – the constraints to ensure the product works well are that the data gathered and placed into Splunk Enterprise is in accordance with the MITRE ATT&CK database in terms of the categories of tactic types, technique names and ID’s, as well as descriptions. More information is provided in section 2.7.1.3.

2.6 User Documentation

2.6.1 - Instructions for Product Use

Instructions for using the product can be found here

2.6.2 - Attack Categorization Information

While there is no interaction directly with MITRE ATT&CK, the scales and categorization used by the system and product are based on the MITRE ATT&CK Database: https://attack.mitre.org/datasources/

2.6.3 - Splunk Integration

Splunk Enterprise will be used as the primary database/area for data to reside. This data will contain detection information and MITRE ATT&CK data. Splunk Enterprise will also be the platform for the visualization tool that this product is created for.

2.7 Assumptions and Dependencies

2.7.1 Assumptions:

2.7.1.1

The MITRE ATT&CK Database will be used to classify the cyber-attack's information about the various cyber-attack tactic categories and techniques for achieving each type of cyber-attack.

2.7.1.2

There is no encryption or decryption processes with the data provided to this product due to this application being integrated within a secure interface and secure system with no outward interactions via the internet or other unsecure channels. Because of this, the fields of the data being analyzed need to be within the Splunk Enterprise system for this application to function properly.

2.7.1.3

The title of the data fields that come from the separate data source – primarily the Kaiser detection system - needs to have the following information and labels:

- *The MITRE name of the technique used. Labeled as "technique".*
- The MITRE ID for that technique. Labeled as "technique_id".
- A timestamp for when the cyber-attack occurred. Labeled as "_time".
- A unique title of the cyber-attack. Labeled as "title".
- A description of what the technique entails, assumed to be from MITRE. Labeled as "description".
- The type of tactic the technique uses, as classified by MITRE. Labeled as "tactic".

2.7.1.4

This product is a visualization tool that resides in the Splunk Enterprise system that is user dependent – meaning that the user must download this application separate from Splunk Enterprise to use it.

2.7.2 Dependencies:

2.7.2.1

Splunk Enterprise will be used to contain and display the cyber-attack(s) data in the card format (Feature 4.1) as a visualization (Feature 4.2 and Feature 4.3) and exporting the data into a PDF report for reporting the attack.

2.7.2.1

The user must have an internet connection with a computer that can run Splunk Enterprise using one of the supported browsers (see section 3.3) in order to access the web page that contains this application.

3. External Interface Requirements

3.1 User Interfaces

When this visualization product is selected it will do the following.

3.1.1 Splunk Enterprise’s Visualization display will display queried data – the cyber-attack data that the cyber-analysist user wants to see visualized – in the “card” format (Feature 4.1) and have it displayed in either the Tactic Priority view (Feature 4.2) or the Timeline Priority view (Feature 4.3) with the Tactic Priority view being the default display with no additional input from the user.

3.1.2 The user can then go to Splunk’s Formatter option, and via a button-selection can select either the Tactic Priority view (Feature 4.2) or the Timeline Priority view (Feature 4.3).

3.1.3 The user can interact with Splunk Enterprise’s Formatter tool to select a color selection window which will create a drop-down menu list of the tactic category colorizations and enable the user to select different colors than the default colorations established for each tactic category. These colors will affect how the cards (Feature 4.1) are displayed in either visualization (Feature 4.2 or Feature 4.3). The default color of the tactic is also in the selection, allowing the user to change the colors back to default colorations from what colors they’ve selected.

Style Details:

Current Default Coloration for the Tactic categories:

Tactic Name:	**Tactic Color Hex-Code:**	**Tactic Color Example:**
Reconnaissance	#f9e98e	🟨
Resource Development	#ffd060	🟨
Initial Access	#ffc336	🟨
Execution	#ff9946	🟧
Persistence	#f28123	🟧
Privilege Escalation	#e06e11	🟧
Defense Evasion	#d1580d	🟧
Credential Access	#ff9595	🟥
Discovery	#ff6e6b	🟥
Lateral Movement	#ff5753	🟥
Collection	#fe3e39	🟥
Command and Control	#fc0607	🟥
Exfiltration	#db0202	🟥
Impact	#c71818	🟥

3.2 Hardware Interfaces

This software is intended to be used with either a desktop or laptop platform that supports Splunk Enterprise. As a Splunk Enterprise application, the software will work on personal computers with Windows, Apple Mac, and Linux/Unix hardware so long as it aligns with the Splunk Enterprise 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 Enterprise visualization application. As such, it will require the cyber-analyst user to have an installation of Splunk Enterprise of version 9.1.1 or higher. The primary method to interface with the application will be via the Splunk Enterprise Web page, which acts as Splunk Enterprise's Graphical User Interface. This will require the cyber-analyst to utilize Chrome, Firefox, Safari, or Edge, which are all compatible with Splunk Enterprise. Additional information on Splunk Enterprise Requirements can be found here: https://docs.splunk.com/Documentation/Splunk/9.1.1/Installation/Systemrequirements

3.4 Communications Interfaces

The communication interface between this product and the data it uses is through Splunk Enterprise. As such the data that is being analyzed must come from a different source and the cyber-attack detection data must be uploaded to Splunk Enterprise which contains the following fields: tactic category, technique name, technique ID, time of the cyber-attack, the custom title of the cyber-attack, and description of the cyber-attack. The tactic category determines the type of cyber-attack and its severity as defined by the MITRE ATT&CK classification, the technique name and ID is the MITRE ATT&CK name and ID that identifies the cyber-attack, the timestamp is the time of the attack, the custom title is the label of the attack instance, and the description contains the description of the cyber-attack's technique in accordance with the MITRE ATT&CK's data on that cyber-attacks technique. All communications of this product are internal and only within Splunk Enterprise – any other sources of communication such as the internet or external systems outside of Splunk Enterprise do not apply to this product as it is assumed this application is within a secure system with no such communication as put forward earlier in this document (Section 2.7.1.2).

4. System Features

4.1 System Feature 1 – Cards

Note: Currently Functioning

4.1.1 Description

The function of the card feature is to display the user-queried data—that comes from the Kaiser detection system and has been placed into a Splunk Enterprise database—on the product's primary visualization window in a card format. The card displays each cybersecurity attack technique as its own card, which 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, the title (an instance label of the attack), and the date and 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 date and time of the attack, the name of the attack's technique, the corresponding technique ID, type of attack, and a unique title for the 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, either a card in its corresponding tactic's deck, or based on its timestamp, depending on which view the cyber-analyst user has selected (Features 4.2 and 4.3).

When a card is displayed to the screen, the cyber-analyst user has the ability to hover over it, which will bring up all relevant information for that card.

4.1.3 Functional Requirements

4.1.3.1:

Each card will be populated using the data obtained from the Kaiser detection software for each incoming attack.

4.1.3.2:

Each card contains the following information:

- The MITRE name of the technique used.
- The MITRE ID for that technique.
- A timestamp for when the cyber-attack occurred. Current time/date format is YYYY-MM-DD HH:MM:SS +00:00.
- A unique title of the cyber-attack.
- A description of what the technique entails, assumed to be from MITRE.
- The type of tactic the technique uses, as classified by MITRE.

4.1.3.3:

Each card will show a concatenated overview of the full data to the user when displayed on the main dashboard. This overview includes the name of the technique used and the timestamp for that attack.

4.1.3.4:

If the user hovers over a card with their mouse, the card will expand to display all the information present within the card and their mouse pointer will be the point from which the card expands.

4.1.3.5:

If there is missing information for an attack technique coming from the Kaiser detection software, the card will still be visible, and the available information will still be generated for the card.

4.2 System Feature 2 – Tactic Priority View

Note: Currently Functioning

4.2.1 Description

The function of this feature is to organize the display of technique cards (Feature 4.1) by each cyber-attack's tactic category 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 displayed to the screen in a column with other cards that belong to the same cybersecurity tactic grouping. Each column will then be displayed on the visualization's timeline, allowing the user to hover over each card and view the full information for each attack. This allows the cyber-analyst user to visualize a cyber-attack by using the visualization window to see what types of attacks are being detected and the severity of the attacks being conducted.

4.2.2 Stimulus/Response Sequences

The formatting menu for the visualization will feature a "toggle" to switch between the Tactic Priority view (Feature 4.2) and the Timeline Priority view (Feature 4.3). The user – the cyber-analyst – will interact with the toggle which will swap from the Tactic Priority view (Feature 4.2 - this feature) which is the default view, to the Timeline 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 columns based on the category of tactic each technique uses and placed onto a timeline.

If the application is in the Timeline view (Feature 4.3), when the user triggers the toggle, the cards will go from the arrangement of the Timeline view (Feature 4.3), back into the columns of the Tactic view (Feature 4.2 - this feature).

When the Tactic Priority view is selected, the cards belonging to a tactic for all available tactics from the queried dataset will be displayed jn the visualization window. A singular card can be hovered over, which will cause the card to expand and display the card's full information: the technique name and ID, the type of tactic used, a unique title, a description of the attack, and the time the attack took place as put forth in Feature 4.1.

4.2.3 Functional Requirements

4.2.3.1:

When utilizing the Tactic Priority view, each card will be placed into a column with all other cards corresponding to the overarching tactic category that their technique belongs to.

4.2.3.2:

When in the Tactic Priority view, each card will initially display the title and technique associated with its given cyberattack.

4.2.3.3:

Each tactic column will display the full range of cards represented in the dataset which are part of that tactic category.

4.2.3.4:

Once a card is hovered over with the mouse, the entirety of the card's information must be displayed: the technique, technique id, tactic, title, timestamp, and description. Once a user hovers their mouse outside of the card, the pop up featuring the card's full information will disappear, and the view will return to its previous state.

4.2.3.5:

The Splunk Enterprise formatting menu for this application features a toggle to switch between the current view, which can either be the Tactic Priority view (Feature 4.2 - this feature) or the Timeline Priority view (Feature 4.3). If the toggle is used from the Tactic Priority view (Feature 4.2), the cards will be sorted into the Timeline Priority view (Feature 4.3). If the toggle is used from the Timeline Priority view, the cards will be sorted back into the tactic columns as put forth by requirement 4.2.3.3.

4.3 System Feature 3 – Timeline Priority View

Note: Currently Functioning

4.3.1 Description

This feature is to represent the card feature (Feature 4.1) for the cyber-analyst user intending to analyze cyber-attack data – which is gathered from a separate detection system, placed into the Splunk Enterprise database, and queried by the user in Splunk Enterprise. When the user decides to use this Timeline Priority view, it displays the technique cards (Feature 4.1) and organizes the cards chronologically along a timeline by the timestamps associated with the cyber-attack data in the cards for the time of the attack. The timestamps are given by reported data from a detection system along with other data associated to the cyber-attack information, including the tactic category, technique name, and technique ID of the cyber-attack. This allows the user the ability to see the cyber-attacks' information such as the tactic categories and techniques that are being used as the attack continues.

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 is a toggle tool in Splunk Enterprise's formatter menu that will enable the swapping of views between the Timeline Priority view (Feature 4.3 - this feature) and the Tactic Priority view (Feature 4.2). The user will interact with the toggle, and it will swap from the Tactic Priority view (Feature 4.2), which is the default, to the Timeline Priority view (Feature 4.3).

The cards from the available data, that has been queried by a user, will then shift in accordance with the timestamps in increments of time referred to as granularity – this granularity will change how the cards are stacked by the amount of time the data covers as put forth by requirement 4.3.3.3. When the toggle for the view is interacted with once more it will swap from the Timeline Priority view (Feature 4.3) back to the Tactic Priority view (Feature 4.2).

4.3.3 Functional Requirements

4.3.3.1:

Will base all information off the timestamps given by the data associated with the cyber-attacks from the data collected from the detection system and placed into Splunk Enterprise.

4.3.3.2:

Will display the data in the form of cards from the card feature (4.1).

4.3.3.3:

Display available cards in the given time-view granularity. Granularity refers to the amount of time the data being queried extends over – this alters where the cards are placed on the timeline as each granularity can cover different amounts of time.

4.3.3.3.a:

If the data being examined extends over a month – the granularity will be that of four (4) 7-day slices of time where the cards (Feature 4.1) are organized into four card “stacks” that will contain the technique cards that occur over the course of each 7-day period starting from the initial time of the first chronological card.

4.3.3.3.b:

If the data being viewed extends over a week – the granularity will be that of seven (7) 24-hour slices of time where the cards (Feature 4.1) are organized into seven card “stacks” that each have the technique cards from each 24-hour period.

4.3.3.3.c:

If the data being viewed extends over a day – the granularity will be that of twenty-four (24) 1-hour slices of time where the cards (Feature 4.1) are organized into twenty-four card “stacks” that each have the technique cards from each 1-hour period.

4.3.3.3.d:

If the data being viewed extends over an hour – the granularity will be that of sixty (60) 1-minute slices of time where the cards (Feature 4.1) are organized into sixty card “stacks” that each have the technique cards from each 1-minute period.

4.3.3.4:

A toggle in Splunk Enterprise’s formatter tool that changes the view from Tactic Priority view (Feature 4.2) to Timeline Priority view (Feature 4.3). That same toggle swaps the Timeline Priority view to the Tactic Priority view if the Timeline Priority has already been selected.

4.3.3.5:

A scroll bar on the Timeline view that enables the view of the cards in a linear and chronological fashion.

4.3.3.6:

Display the cards 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

Note: Minimal Functionality (was dropped in 2023 and other items took precidence)

4.4.1 Description

This feature would allow the ability for the cyber-analyst user to use Splunk Enterprise's export tool to print a report of the data to a PDF file. This file contains visualization of the data from the current view – either the Tactic Priority View (Feature 4.2) or the Timeline Priority View (Feature 4.3) – and the data that the visualization shows.

4.4.2 Stimulus/Response Sequences

The cyber-analyst user interacts with Splunk Enterprise's printing tool 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: the visualization seen by the user, and a list of the items in the visualization.

After generating the report, the user will interact with the rest of the Splunk Enterprise's printing tool to confirm the report. 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

4.4.3.1:

The items necessary to export the visualization to Splunk Enterprise's printing tool need to be provided to Splunk Enterprise.

4.4.3.2:

The ability to use the visualization tool's data and print that data into a report.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

5.1.1

Performance Requirement #1: The software needs to be able to handle at least several months' worth of cyber-attack detection data and process it into a visualization.

5.1.2

Performance Requirement #2: The product is intended to run on Splunk Enterprise's systems and thus must be able to run on the systems that Splunk Enterprise operates on.

5.2 Security Requirements

5.2.1

Security Requirement #1: 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.

5.2.2

Security Requirement #2: This software could contain information important to the cybersecurity of Kaiser Permanente, and extra steps should be taken to safeguard this data. This product's purpose is not to safeguard or protect specific data. And as such, this group does not hold any responsibility for the data analyzed with it or the security for the data as this product is intended to be used in an already protected system and not go outside that given system. It is on the users of this product to provide the data this product uses.

5.3 Software Quality Attributes

The current software quality attributes emphasis visually pleasant design which is interpreted as:

- Having minimal buttons (less than 5).
- Having accessible information (less than 10 clicks or actions to get to any given feature).
- Having a design that has good coloration for both information display and aesthetic purposes. Such as:
    - Cards (Feature 4.1) having a color hue range from yellow to red depending on severity.
    - Having a background color that allows for the information to be clearly seen.
- Data being displayed in less than 10 seconds from the user running a query.
- Having a notification for loading or errors.

Appendix A: Glossary

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

Card stacks or *stacks* – this is a reference to system feature 4.1 and how the feature displays the data in columns.

Tactic or *Tactic category/categories* – The most abstract description of the type of cyber-attack. Each technique of cyber-attacks belongs to one or more tactic categories that are classified by the MITRE ATT&CK database which defines the cyber-attacks goals, objectives, and severity.

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 being placed along a horizontal axis.

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

Card Data, *Data*, *or Intended Data* – This refers to the data that this product is intended to operate with. This is cyber-attack data that includes the data fields of:

- The MITRE name of the technique used.
- The MITRE ID for that technique.
- A timestamp for when the cyber-attack occurred.
- A unique title of the cyber-attack.
- A basic description of what the technique entails, assumed to be from MITRE.
- The type of tactic the technique uses, as it is classified by MITRE.

Visualization – This refers to the visual display in Splunk Enterprise which is used to display data in either a custom fashion (Feature 4.2 or Feature 4.3) or the default graphics within Splunk Enterprise.

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 and the navigations that are wanted or desired.

Need to further develop the Cards (Feature 4.1) for sorting the techniques by Tactic categories – primarily the color and style since there are 14 tactic types and distinguishing between the tactics is needed for product functionality.

Need to further develop the Performance requirements.

Need further information on the Software Quality Attributes such as ease of navigation or what “visually pleasant design” means to the client and the users.