Kaiser Permanente Cybersecurity Project – Client Meeting Summary:

**Participants:** Danae O’Connor, Noah Warren, Bailey Hughes, Debra Parcheta, Vuong Tran

**When:** 11:00am to 12:00pm on 9/20/2023

**Where:** <https://ucdenver.zoom.us/j/9681646314> Meeting ID: 968 164 6314

**Summary:**

The three primary points of discussion were the conformation of existing contact methods (email with a text), a review of the primary system features in the Requirements document for this project in broad terms, and the discussion of key questions to form a starting point for this product and clarification of details regarding data being used and the Splunk application and how it is to be used.

**Discussions & Details/Conformations:**

Contact methods of email and text work.

The system features of the requirements document are currently approved but do need refinement. The Card feature is the central feature, while the tactic and timeline features are also wanted with a way to toggle between tactic and timeline. The report functionality is also wanted with the ability to export out to a PDF with the following information: Visualization of the current data and a list of the data items in the display – the data should be listed in the accordance with the view at the time of report generation (tactic listing in the Tactic view, chronological listing in the Timestamp view).

Answers to questions:

* This product will be a Splunk application and will primarily be a visualization tool for data.
* The data for the product will be within the Splunk database for when it is released, however, for testing purposes the data will be in the form of a CSV file with the needed information of tactic, technique, timestamp, and description. Primarily need to create a query to get the correct information from a larger system.
* Card data is confirmed to have tactics, techniques, timestamp, and description as the necessary components. Discussion of color will be held at a future date due to it being tied to functionalities of the application.
* The testing data will be available to us by 9/22 or within the next week.
* The intended users are cyber-analysts to give a visual representation of the attack.
* The application is to be primarily used during an attack, but it should be able to view old(er) data or the data of the attack after the attack has happened for analysis and be able to report on it.
* Logins and other identifying items are not needed as that will be determined by the Splunk admins at Kaiser when the application is integrated into the system.
* The GitHub will become public – however the end intent is that it will be published on Splunkbase, which is Splunk’s application area, so there isn’t a need to hide the GitHub. The link will be provided in a later email.

The next meeting will be held in person at the Tivoli Starbucks on Tuesday 9/26 at 6:30pm - 7:30pm.

**Additional:**

Make sure to use the CIM (Common Information Model) in order to query items. Documentation on Splunk can provide more information about Splunk and its capabilities. D3 is a JavaScript visual library which can aid in the creation of the application’s visualization.

Recommended action for team is to download a Splunk app – especially a visualization tool – in order to gain a better understanding of the capabilities of a Splunk application.

**Action Items for 9/20 to 9/26:**

Vuong – Create or get tester data preferably done by 9/22, or 9/29 at the latest.

Debra – No actions needed at the current moment. Review Splunk items if schedule allows. No due date.

Danae – Study Splunk regarding databases, data, queries, and visualization tools. Due 9/25.

Revising Requirements document. Due 9/26.

Aid in base application and GitHub setup 9/26.

Noah – Study Splunk regarding databases, data, queries, and visualization tools. Due 9/25.

Making the GitHub Public. Due 9/22.

Create initial base application. Due 9/26.

Bailey – Study Splunk regarding databases, data, queries, and visualization tools. Due 9/25.

Revising Requirements document. Due 9/26.