Kaiser Permanente Cybersecurity Project – Team Meeting Summary:

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

**When:** 11:00am to 12:00pm on 9/18/2023

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

**Summary:**

Met with the entire team. Discussed that as of right now we need to talk to the client, Vuong, to ensure that we make the product in the correct place – either in Splunk as a dashboard like or in a separate webpage. Also concluded that some important questions to ask are whether the test data we will be given is to represent data from a detection system in a separate database or if the product will be expected receive and store information. In addition, does has the data already been classified as in the Mitre format.

Those working directly on the project need to continue learning about Splunk and its abilities as well as overviewing the Mitre Att&ck database.

Discussed swapping over to Jira as our primary progress tracking tool – but issues may occur so it should be willing to be dropped entirely. As such, the Excel spreadsheet for the Gantt chart will be the primary progress tracker until either a full swap to Jira can be made or if the Jira system fails so we still have a way too track our progress and keep moving.

**Issues:**

Need to ask Vuong the following questions to start building the product:

* Is this product made to be Splunk only or is this expected to go on a separate webpage with Splunk?
* Is there a detection system that drops data into a database for this product to monitor or is the product expected to have data pushed into it?
* Is the data being given to the product classified with the Mitre datatypes?
* How soon can we get the testing data?
* Does this product need the ability to log-in?
* Is there a minimum amount of time you want to see the data at? [For Card stacking abilities.]
* Would you or others want access to the GitHub we are working with?

**Additional:**

Depending on outcome with client will result in first batch of work being assigned. Who is doing the primary integration with Splunk and Mitre – if it needs to be a team effort. Who will be constructing either the domain names or the dashboard to implement. And who will be designing the start of what interfaces so that databases can be constructed and plans on how to fill them with information can be started.

**Action Items for 9/18 to 9/22:**

Danae – Set up Jira (Due by 9/22), upload files to the GitHub (Due 9/22), Splunk Tutorials, Mitre data review (Due 9/20).

Noah – Splunk Tutorials, Mitre data review (Due 9/20). Join Jira or tell team lead (Danae) that this will not work (Due 9/22).

Bailey – Splunk Tutorials, Mitre data review (Due 9/20). Join Jira or tell team lead (Danae) that this will not work (Due 9/22).

Debra – Check for emails that allow access to the GitHub we are working with (Due 9/22). Join Jira or tell team lead (Danae) that this will not work (Due 9/22).