Kaiser Permanente Cybersecurity Project - Meeting Agenda:

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

**When:** 11:00am to 12:00pm on 10/4/2023

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

**What is being covered:**

Other than the title field needing to be added to the document were there any other issues that concerned you or you think need to be addressed?

For the title field – roughly what will be in the data? Is it tied to tactic or technique in some way?

We need to confirm that the data – for production – is either streamed data being fed into Splunk or if it is going to be in some kind of file. This could be needed for queries.

In addition, since this is to view a cyberattack, are there any delimiters that would mark the start or end of an attack? Or will that be determined by the user?

While exploring the query function in Splunk using only the data you gave us we came across a potential issue – but we are unsure if it is a query issue or something else. By using the following query, we picked up 34 tactic fields. Is this intentional or is this data that will be needed to be sorted by our system?

The query used is as follows:

| inputlookup cu\_denver\_data.csv

| stats count by tactic

We will be overseeing several beginning mock-up designs in order to get a better understanding of what you want.