Kaiser Permanente Cybersecurity Project – Team Meeting Summary:

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

**When:** 11:00am to 12:00pm on 9/25/2023

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

**Summary:**

Team met. Discussed the testing data – the non-cleaned version given to us on Friday 9/22. Need to be particularly wary of the timestamp field and how Splunk handles timestamps and indexing timestamps, as well as ensuring that the tactics, techniques and the tactic ids are valid and line up with the MITRE testing data.

Conducted a Splunk Study session in order to dive into data importing/uploading into Splunk, querying, and visualization creation.

**Issues:**

Ensure that the data being used is cleaned properly.   
Double check with Vuong for how the “time” field is classified by the detection system: Is the timestamp given by Splunk or is it given by the system? This is needed to know due to how Splunk gives timestamps depending on when the data was inputted but there is a timestamp field that is either when Splunk indexes it or when it actually happened.

**Additional:**

No additional items.

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

Danae – Splunk information gathering, and Requirement Document edits (9/26).

Noah – Splunk information gathering, and Requirement Document edits (9/26).

Bailey – Splunk information gathering, and Requirement Document edits (9/26).

Debra – No action needed at this time.