For our mockup prototype, we have designed the user interface for our webapp. It includes the following sections: login page, activity display, aggregated activity display, activity details display, user activity history display, and alert list. We used proto.io to implement a simple mock-up UI prototype. The prototype can be found at product_research/UIUX/: Open index.html in a browser to view prototype.

UX Experiment

We asked two potential users, who have never seen our prototype, to use our prototype for our UX research study. The purpose of the experiment is to make our product more intuitive and easy to use. Without any guidance or information on how to use the product, we asked the interviewees to complete certain scenarios and observed how they interacted with our prototype. We have reached out to a software developer who has experience and knowledge in UEBA and a front-end developer in analytics visualization with related project management experiences. Each person was interviewed individually and were given the same scenarios.

Scenarios:

- Log in using given credentials: username “dtect”, password “123”
- Find out how many logged events were authentication activities
- View activities list within one specific timeframe
- Check the details of one non-suspicious activity
- Check the details of one suspicious activity and the corresponding user’s activity history; check the details of this user’s one other activity
- View a past alert and the details of that alert

The raw notes can be found in the “raw notes” section. Here are the key takeaways from our observations:

- Keyboard shortcuts are commonly used especially when typing is involved (eg. when logging in pressing “tab” to go to next field, and pressing “enter” to complete login was common)
- Areas that are clickable should be obvious and indicated. A few clickable areas cause the users to perform unnecessary moves(e.g. Clicking on the user value on the activity table to access the user profile, the prototype brings up the log entry description instead)
- Tables and charts should not only display information cleanly, but also be interactive (eg. clicking on a domain in an event log table will bring up the domain’s description)
- Colors and shapes should be used strategically to imply certain meanings for better intuition (eg. red entries means flagged, green means non-suspicious)
- Data displayed should be as human-interpretable as possible (eg. User ID versus User name)
- “Do more with fewer clicks”: minimize the amount of pages required to navigate to get the desired information

Feedback

We have had insightful and constructive feedback from our UX experiment participants. One of the common feedback was to enable filtering/sorting/searching features for the display of past events. All feedback can be found in the raw notes included. These points are discussed and integrated into our roadmap for upcoming weeks of UI development.

Improvements

Here are features we intend to implement which were not positively reflected from our mockup and the UX experiments.

- The option for users to ignore alarms and label activities as non-suspicious.
- Include keyboard shortcuts for login page (“enter” instead of pressing login button)
- Make accessing the information of a certain timeframe more intuitive
    - Rename timeline chart instead of “Date histogram”
    - Add highlighting feature to the timeframe when section is hovered over
    - Improve visuals to differentiate the chart from simply a data plot
- Change event list appearance
    - Instead of labelling individual logs as suspicious or not, label groups of logs, perhaps by user and/or more specific timeframes (maybe the size of a timeframe being sent to the model)
    - Indicate the row can be clickable but not make the user think each entry in the row leads to something else
    - Filtering, sorting, searching features
    - When clicking on sections of the aggregation chart, filter event list by the category
- Change colour of non-suspiciousness (currently mixed with the colour scheme of the web page)
- In event detail page, change user ID to user name
- Change detail page from the form of a pop-up window
- Add a button that leads to a list of all users

Based on the UX experimentation and feedback we have updated our roadmap, project board, and milestones, and will continue to update them as the development progresses.

Raw Notes

Person 1 (role: software dev who knows about ueba)

- pressed “enter” keyboard input to complete login
- had trouble using timeframe chart to access aggregated logs within timeframes
- had trouble accessing user activity history through the log details
- noticed that logs with red text means flagged activities and green means non-suspicious
- noticed that clicking on a row would lead to details of the log entry
- spent some time finding out which areas of the screen were clickable
- in history, does not know which activities were seen
- sort by columns by clicking on table column

- when clicking on a user of a event log row entry, person expected to see details of the user rather than the details of the event
- label groups of activities (events) by timeframe
- filter by event type
- suggested to make flag groups of events as suspicious rather than individual events (eg. one failed authentication may not be suspicious, but 10 failed attempts might be)

Person 2 (role: has front end dev in analytics and project management experience)

- Pressed tab after entering username but cursor doesn't change to next text box
- Had trouble finding user activity history: made multiple attempts to click on username in table to see user history

feedback

- filter by pie chart info (activity type or domain etc)
    - Pie chart should change based on the timeframe chosen
- search function for logs
- make logs smaller
- show logs from multiple desired timeframes
    - Add date selection
- advise not to lead a pop up to a second pop up (instead, show details as panel to the side or whole page with back button)
- suggested to have advanced filtering such as seeing logs of a specific user from a certain time of day on certain days (or past few days)
- Repeated scheduled queries for people who like to run queries during certain times
- Saved filtering options would be a good idea for users who like to use the same filtering options