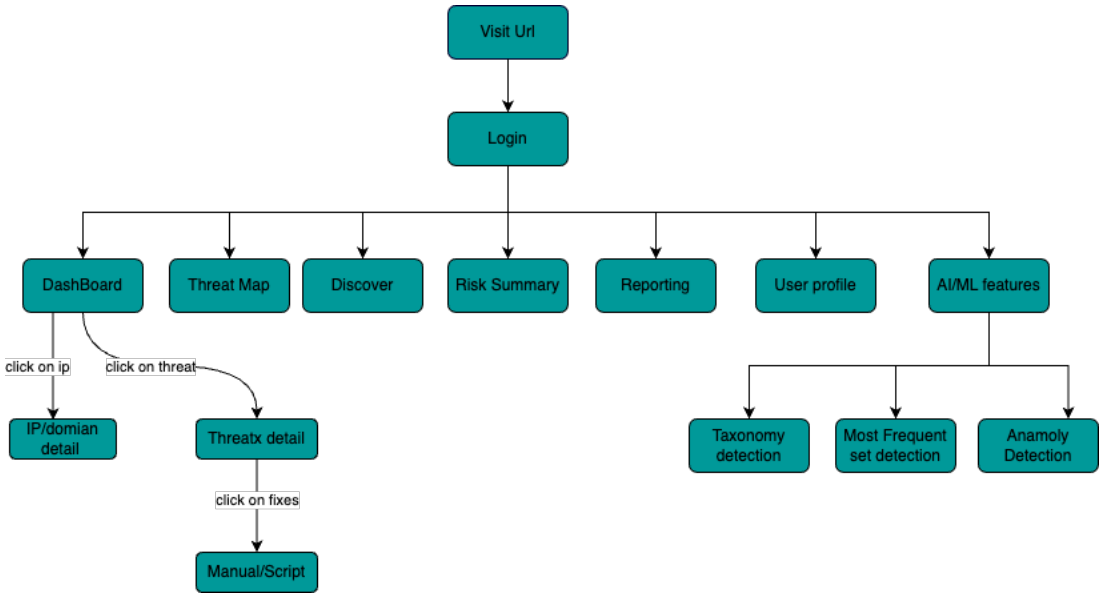
DTM Flow diagram:



1. **Login:**

   In order to log in, users are asked to provide their username and password in the designated fields.

   Incase users have forgotten their password they can reset it by clicking the "Forgot Password" link. Upon clicking this link, users will be prompted to provide their email address in order to get instructions on how to reset their password via email.

2. **Dashboard**

- Visualize Data:
  - Enables the Creation of various types of visualizations such as line charts, bar charts, pie charts and more, using the threat data extracted from the database. These visualizations should help gain instant insights threat facing an organisation, identify trends, patterns, and outliers.

- Interact with Visualizations:
  - Visualizations also needs to be interactive, allowing users to drill down into data, filter results, and explore specific aspects of the data in real-time. This interactivity enhances the analytical capabilities of dashboards.

2.1. IP/domain details

2.1.1. This page should be dynamically generated based on the IP address or domain a user clicks on in the dashboard.

2.1.2. For instance, if a user clicks on specific ip, it should highlight all events related to that ip likewise for specific domain.

2.2. Threat Details

2.2.1. It will display more details on certain kind of threat a user clicks on dashboard, such as indicators of compromise (IOCs), known malicious IP addresses, domains, file hashes, or URLs with a link to manual and script.

2.2.2. Manual/Scripts:

This page will have the technical manuals with step-by-step explanation on how to verify the detected threat, clean and mitigate the risk. It will also include scripts to automate the process where applicable.

3. Threat Map:

3.1.1. This page is a visualization that displays geographic information about security threats, incidents, or events on an interactive map. This visualization is particularly useful for understanding the geographical distribution of threats, identifying hotspots of malicious activity, and visualizing the global impact of security threats that are affecting an organisations environment.

4. Discover page:

4.1.1. Search and Explore Data:

Search and explore the data imported from threat database such as searching for specific terms or phrases, filtering data based on various criteria, and examining the raw documents with a user-friendly interface.

4.1.2. Time Series Analysis:

Enables to visualize and analyse data trends over time with features such as specify a time range and zoom in or out to focus on specific intervals.

4.1.3. Field Analytics:

Provide insights into the fields present in the dataset, including data types, cardinality, and distribution. This helps in understanding the data structure and identifying anomalies or patterns in the threat data.

4.1.4. Interact with Data:

Ability to interact with the search results, such as selecting fields to display, sorting data, and aggregating metrics to enable a flexible and customizable analysis experience.

4.1.5. Save and Share Queries:

Ability to save queries for future use and share them with colleagues to promote collaboration and ensure consistency in analysis.

5. Risk Summary

5.1. Risk Score:

A graphical representation of the organization's overall risk score, which is calculated based on a combination of factors such as the severity of identified vulnerabilities and attacks, the likelihood of it leading to security incidents and other risk indicators.

- Risk Trends:

Visualizations showing trends in risk levels over time, including changes in risk scores, the frequency of threats detected, the effectiveness of risk mitigation efforts, and other relevant metrics. These trends should aim to assist stakeholders track the evolving risk landscape and assess the effectiveness of manuals and scripts applied.

- Top Risks:
  A list or chart displaying the top risks facing the organization, ranked by severity, likelihood, or impact. This section should highlight the most significant threats and vulnerabilities that require immediate attention and remediation.

6. **Reporting**

- Scheduled Reporting:
  Allow users to schedule the generation and delivery of reports at predefined intervals, such as daily, weekly, or monthly. Scheduled reports should be set to be automatically sent via email so the users receive timely updates without having to login to the system frequently.

- Create Alerts:
  Configure means to receive alerts either via sms, email, Slack or Microsoft Teams. This would enable users to receive alerts if either new threat or any anomaly is detected, ensuring timely notification and response to threat in real time.

7. **User Profile:**
   - It should include essential details like name and email, along with preferences such as email frequency and notification settings. Users can manage their account settings, including password management, and define their role within the system, enabling role-based access controls to ensure appropriate data access and security levels based on their responsibilities and permissions.

8. **AL/ML features**

   AL/ML features typically refer to the integration of automated machine learning capabilities for anomaly detection, trend analysis, and predictive analytics. This can include threat taxonomy detection, correlating relations between IoCs with most frequent item set detection and anomaly detection in time series data that might indicate new threat or targeted attack for instance. This will include links to various models integrated into the platform.

   8.1 Taxonomy Detection

   After testing various models on data collected using intelmq, the best performing model will be integrated to automatically detect threat taxonomy derived from other attributes/IoCs.

   8.2 Most frequent set detection

Like wise after testing various association rule mining algorithms, the best performing algorithms will be integrated to detect the most frequently appearing set that might indicate relation between and ip and a malware or vulnerability for instance or even infer a malware identity that is named differently by various providers.

8.3 Anomaly detection:

Similar to earlier machine learning techniques, time series analysis would essentially be helpful to analyse attacks over time to detect new threat patterns and predict future risk.