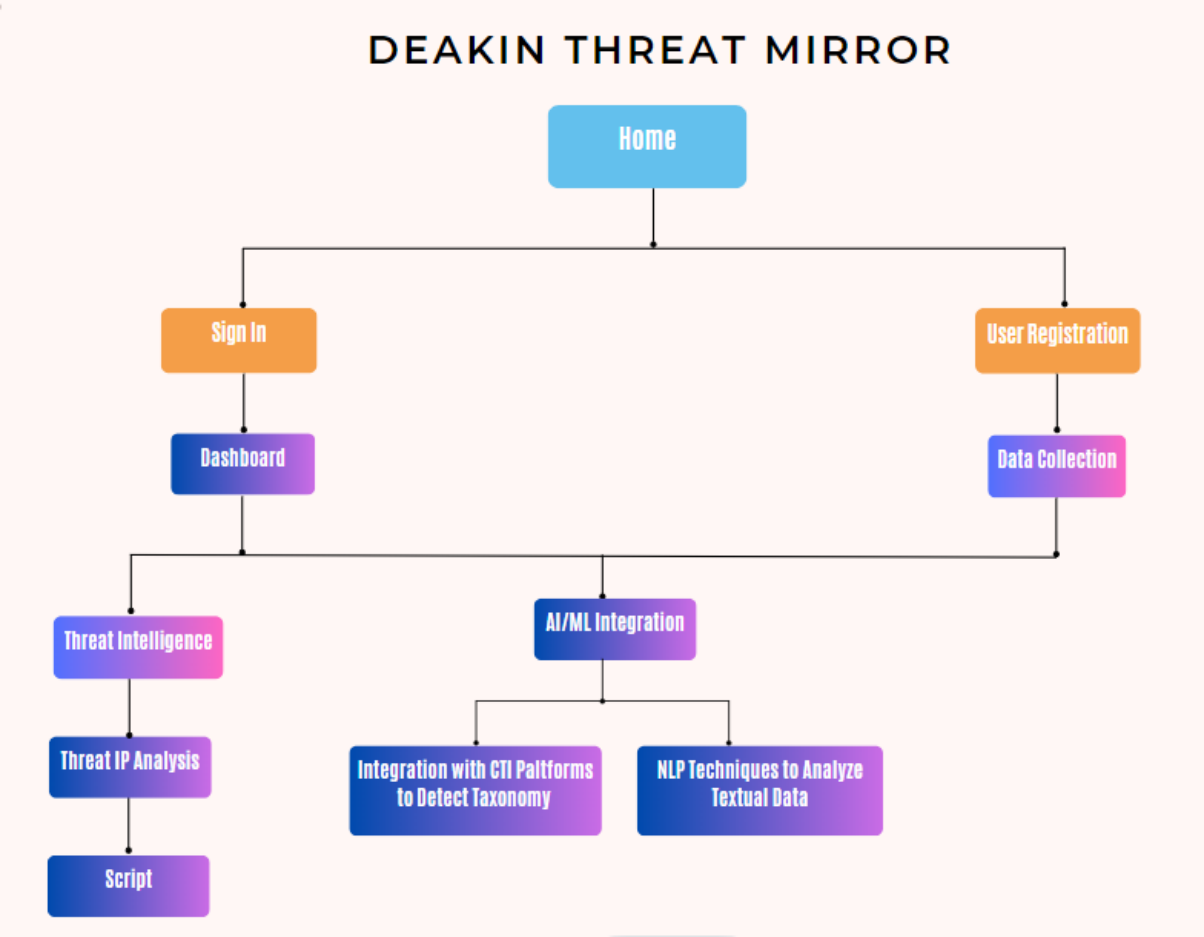
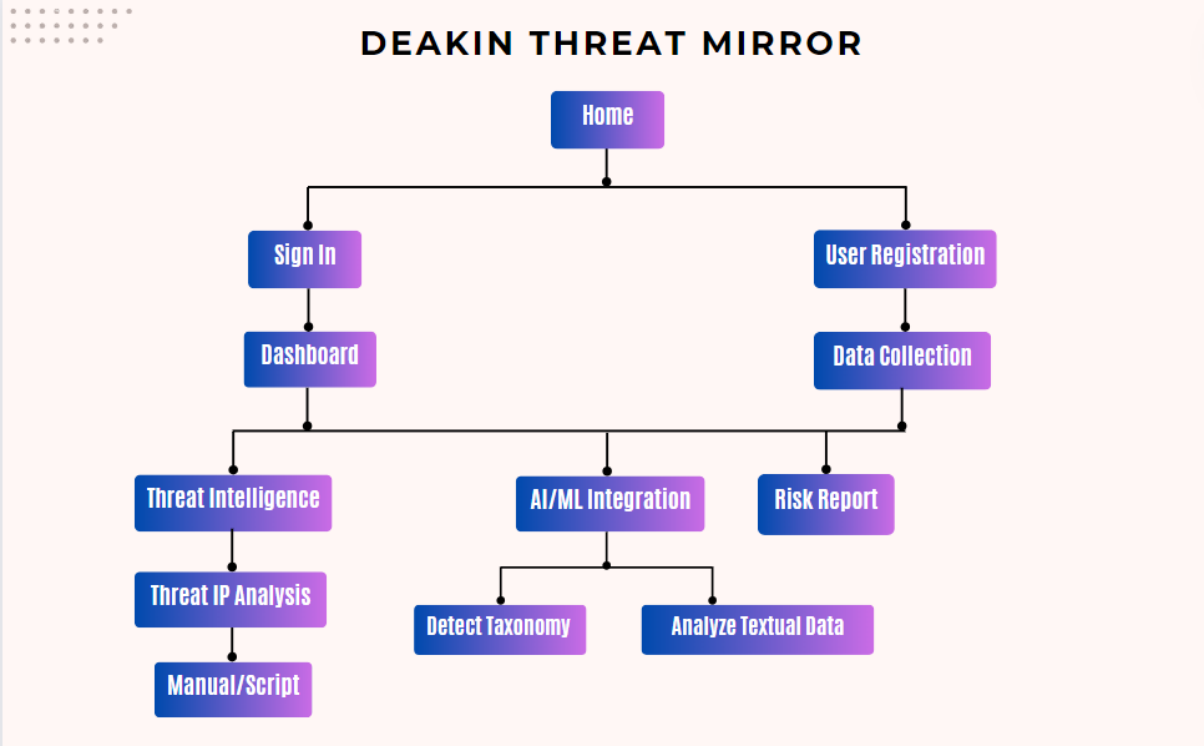
Flow Diagram

Initial Idea:



Final Version:



This flowchart outlines the user interface (UI) flow for the website of the Deakin Threat Mirror project. The idea I have proposed demonstrates the product as a threat intel service which can be run by Deakin and dedicated team. Below here is a breakdown of each page:

- **Home:** The initial page of a website that visitors land on. It offers navigation choices and a project summary.
- **Sign In:** This is the page for users who already registered on our site and can sign in through their credentials.
- **User Registration:** Users can register for a new account if they don't already have one.
- **Data Collection:** This section will focus on collecting data from SMEs and organizations, which will play an essential role for analysis and threat detection. The new users can provide data of their environment and we collect it through our tool IntelMQ.
- **Dashboard:** Following their login, users are taken to the dashboard, which acts as the primary location for gaining access to threat intelligence and AI/ML features and Risk Report.

- **Threat Intelligence:** From dashboard users can navigate to threat intelligence page where there will options for them to utilize threat and IP analysis.

- **Threat IP Analysis:** This part gives users comprehensive information and intelligence about potential risks of IP's or domains and threats. Additionally, if any threat detected such as brute force user can solve the issue by navigating to the next page which is manual/script.

- **Manual/Script:** This component, users can manually intervene or execute scripts to address specific threats or issues identified through threat IP analysis. This could involve taking manual actions to mitigate threats or running predefined scripts to automate certain responses.

- **Risk Report:** Users can use this page to generate a risk report. For example, if a susceptible IP address has malware associated with it, it may be considered a high-risk asset in their environment since it is either compromised or is attacking someone.

- **AI/ML Integration:** By utilizing methods like taxonomy detection and natural language processing, artificial intelligence and machine learning are combined to improve threat detection and analysis. Users can access two different features from here such as taxonomy detection and textual data analysis.

- **Detect Taxonomy:** This component will perform automating threat classification procedures by integrating the taxonomy detection system with our tool IntelMQ. For this, the integration of databases and threat intelligence feeds to add taxonomy labels to threat data.

- **Analyse Textual Data:** This component will apply natural language processing (NLP) methods to textual data analysis about cyberthreats.