**Statement:**

A telecom mission control SaaS platform provides intelligent services for enterprises. Multiple carriers often share cell towers, but not all towers support all carriers. The carriers (AT&T, Verizon, T-Mobile, etc.) determine the devices supported at the towers and the device's operating system (iOS, Android, Windows, etc.). For example, some towers will only allow iOS-based AT&T devices, while others will allow Android and Windows-based AT&T and T-Mobile devices, as well as additional unique combinations. The equipment at the cell tower detects the apps used by the user on their device and captures the actions performed on the app by the user. The system captures the policy determined by the enterprise to enforce the rule, allowing or denying the list of actions permitted on the app based on the user's role. The system provides value-added services such as a real-time dashboard to monitor the security health. A higher subscription plan provides auto-remedial action enforced at the cell towers through enterprise-defined policies to secure the edge. The system integrates with various communications real estate developers to ingest (register) the information related to the towers present nationwide and the carriers they serve. The system allows connecting to different sources for onboarding existing users and their devices. Additionally, the system enables auto-discovery of new enterprise devices through the cell towers.

Architect and design in detail a high-assurance, a11y-friendly, scalable frontend system for web and mobile users used globally in both online and offline modes on devices of different form factors for the above use case. Define and illustrate high-level architecture. Design the data flow models for each feature. Define the API model and design a performant API. Model the entities and their relationships. Do all of this for each feature that I list next

**Module-wise breakdown of UI:**

1. Policy management: The Enterprise users (Policy admin role) can define the rules to apply to the devices held by their employees. The rules to either allow/disallow actions in the apps can be based on any combination of role, location, OS and device type. If the enterprise has opted for a higher subscription plan the user (security analyst role) can also configure remedial actions to take in cases of misuse or malintentions, for example to .

2. Security Dashboard: The Enterprise users (Security analyst role) shall have access to this module. They can see the relevant events captured/acted on by the cell tower. Filters like time, location etc shall be provided . Events could be warnings, alerts and in case of high subscription plan, auto-remedial actionss taken by the system.

3. Device, User, Inventory and Work location management: The Enterprise user (Inventory manager role) can add new users to the system. The user can also add new devices to the system and assign them to a User. The device type can be an item from the device inventory that the Enterprise users have created. The user can create the inventory by adding items from the pre-defined items available to use by the Saas Platform or create their own items. User can create work locations that could be a group of cell towers. User can add/manage new cell towers (accessible to only the enterprise) that are not publicly known either from the UI or file export/import option. A section displays auto-discovered devices that need to be reviewed. Assumption here is that if a device has got access to the network means it has already been authenticated by the enterprise using the SIM profile and their IDP solutions which is not in scope of the SaaS platform.

4. Manage enterprise: Enterprise user (Enterprise admin role) can manage subscription, their users that get access to the SaaS platform also and assign them roles

5. Enterprise onboarding/management: The SaaS platform user (Onboarding specialist role) can create new enterpises, initial enterprise admin user.

6. Tower management: The Saas platform user (Tower manager role) can view and manage the towers ingested by the system. User can also create and manage new towers from the UI or using a file export/import option. A map view shall also be provided.

At a global level the system should take care of below points:

* Offline Data Management that handles local caching, queueing of actions, Sync conflict resolution, and error handling.
* The system should be accessibility friendly,
* should have support for various devices and form factors.
* have i18n support as well.