**Plan:**

* Ingesting data, processing, and applying correlation logic using Python, along with machine learning (for new rules) and rule-based automation (for known rules) for pattern recognition and Root Cause Analysis. Then smart-alerting (routing to the correct stakeholders) and automating remedial actions (EDR, XDR, SOAR). Following is the sequence

1. **Event correlation**
   1. Step 1: Intra data source: We will try clubbing together similar events from one data source to generate minimal number of tickets
   2. Step 2: Inter data source: After step 1, we will try clubbing together similar events from multiple data sources to club different events into one major event.
2. **Rulebook or playbook (Workflow Automation)**: Next, the goal is to automate action steps for events to right stakeholders.
3. **Predictive Analysis:** Lastly, once the first two steps are achieved, we will try to **predict** incidentsbased on incoming logs.

**Dependencies:**

* Examples to understand how our network events from different sources relate to each other. And how does a person manually correlate the events (on what parameters).
  + This is a very important requirement right now. I need to understand some examples of the type of correlations we can do across our specific data. Someone in operations who deals with the log data manually and then identifies Faults/Root causes would be able to guide I assume.
* Network topology: to find out how devices are connected to each other.