# ASSESSMENT PHASE

1. Threat Modelling to be done manually for each device type (subset of techniques)
   Historical probability of a threat is based on past 10/15 year data (if available)
   Simulated Threat Probability can be used in cases of advanced threat alerts
   Currently, simulated probability is based on the number of vulnerabilities per threat regardless of device type.

| Device Type | Threat | Historical/Simulated Probability(H) |
|---|---|---|
| NW/PC/DB/Ser | | |

2. Threat Vuln Map
   Threats - MITRE ATT&CK tactics
   Vuln - NVD CVE list

| Threat (Tactics) | Techniques | Vulnerability |
|---|---|---|
| | | |

3. Vulnerability scanning for each asset type
   Using Nessus or Open source tools like openscap, OpenVAS etc.
   Currently, using NIST APIs to collect vulnerabilities per asset

| Asset ID | Asset | Device Type | Vulnerabilities |
|---|---|---|---|
| | | | |

4. Using threat modelling for that device type, vulnerabilities can be mapped to threats and probability of compromise can be calculated for each asset
   Impact score to be decided by the organisation
   Probability is the function of threat probabilities and number of vulnerabilities used to actualise the threat: $P = \sum H_i N_i$ for each threat

| Asset ID | Impact (out of 10) (I) | Likelihood (P) |
|---|---|---|
| | | |

5. $$R = \frac{\sum I \cdot P}{\sum I}$$