**Production support Monitoring Automation**

**Purpose**:

To do the due diligence of the system which need to be integrated with Elastic search/Splunk framework to automate the production support monitoring.

Scope:

* Draw an overall component diagram with all the interfaces and feeding systems.
* Draw a virtual boundary / scope and identify the target system
* Identify all the sources which emits **alerts** and **logs** and which need to be added in elastic search framework. (Application team)
* The sources should include –
  + Application, Host machine, VMWARE, Filesystem, database, Network, Messaging bus, KEDB, APM tools (AppD, Dynatrace)
* Identify the connecting agents which can be used to integrate (Automation team)
* Identify the primary / secondary owners for each system (RACI matrix)
* Estimate the size of logs / alerts being collected daily i.e. data size and number of alerts
* Identify the spikes in the load
  + Weekly and Monthly
  + Seasonal
  + Regular Campaign / or refers to Statistics of the last campaign
* Identify the e2e business transactions which need to be monitored (Do not confuse this with Application monitoring usecases)
* Identify what need to be monitored at Root level
  + Regular Points of failure – (examples, add more as per the specific need)
    - like Host machine CPU, Memory
    - Network speed (internal and external)
    - Available space on filesystem
    - Availability of the interfaces
  + Business events - (examples, add more as per the specific need)
    - Avg number of records processed by each job
    - Avg | Max number of users by region and by time of year