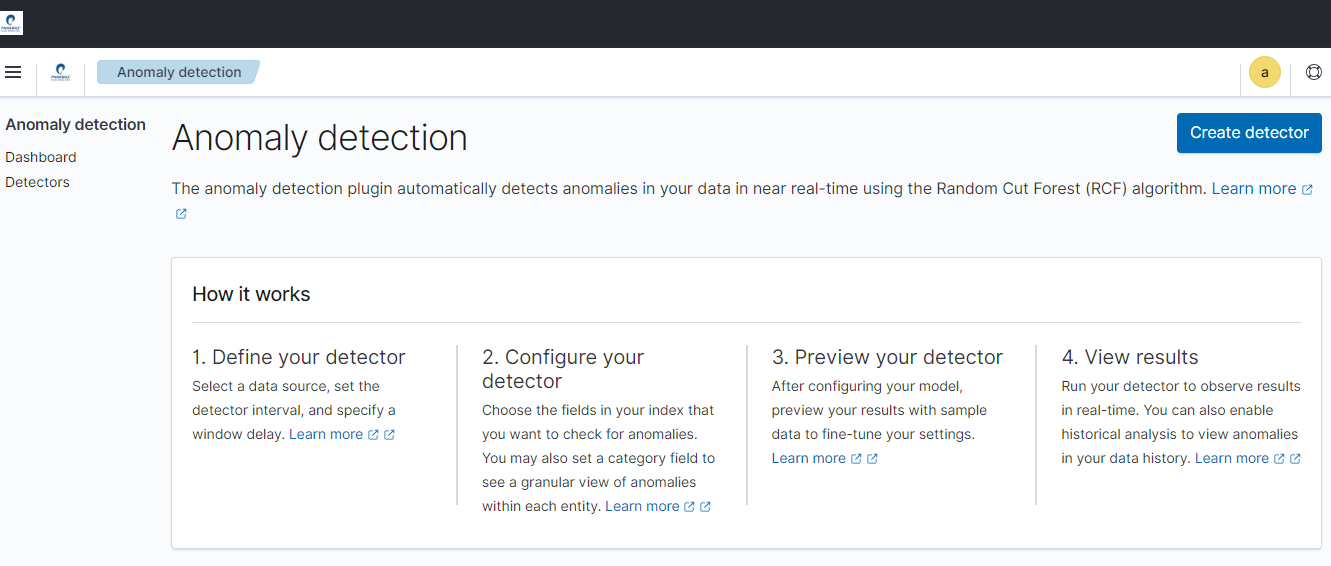
## How to setup alerting and Anomaly detection in opensearch:

Before alerting we need to configured the Monitoring in opensearch by using opensearch dashboard. There are 4 type

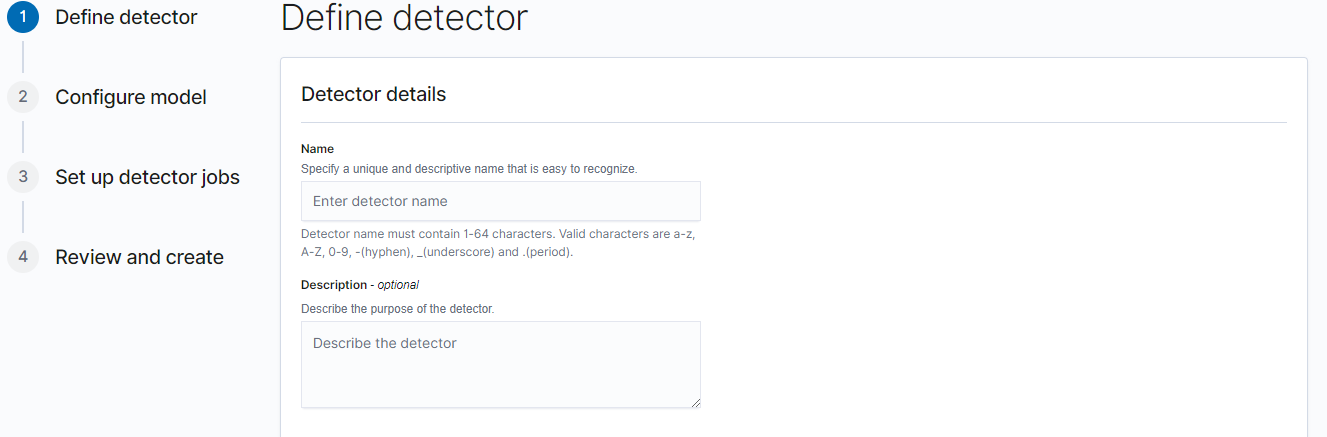
# Anomaly detection

1. Define your detector
2. Configure your detector
3. Preview your detector
4. View results



Detector Settings:

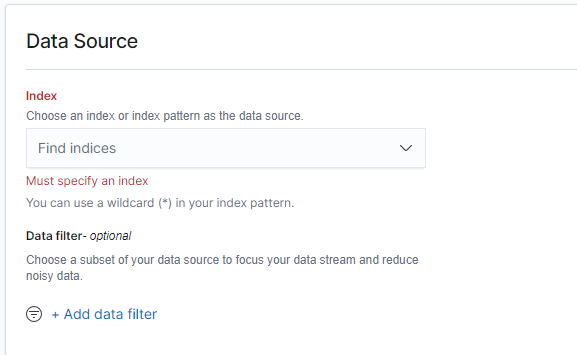
1. Define detector



Name of detector: memory\_detector

Description: memory\_detector

1. Data Source:



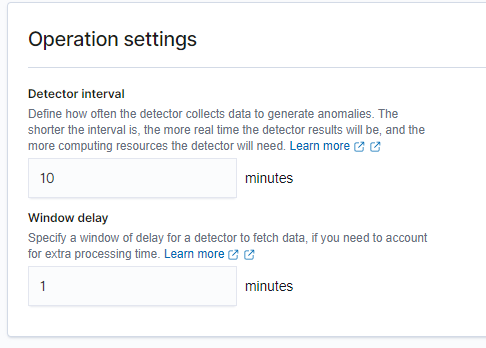
Select index name as metricbeat (metricbeat-7.12.1-\*)

Here we don’t requred the extra filter for anomaly on index. Hence

1. Timestamp:

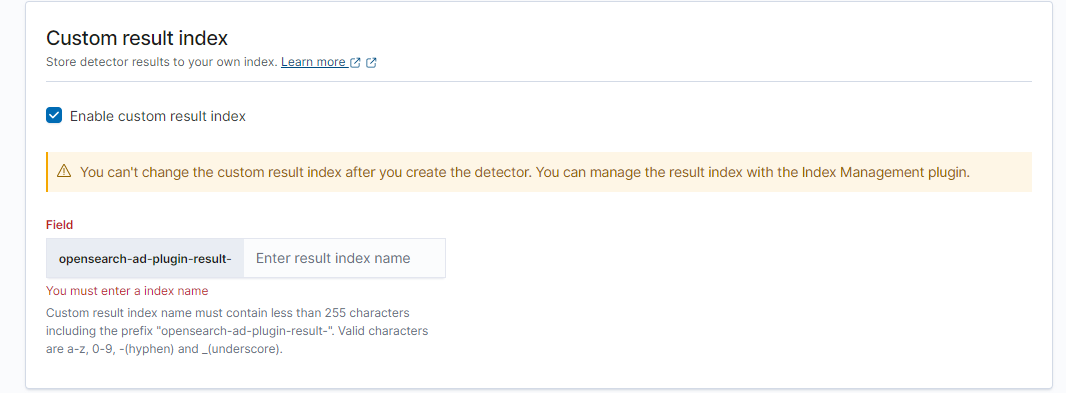
Select timestamp is @timestamp

1. Operation settings:

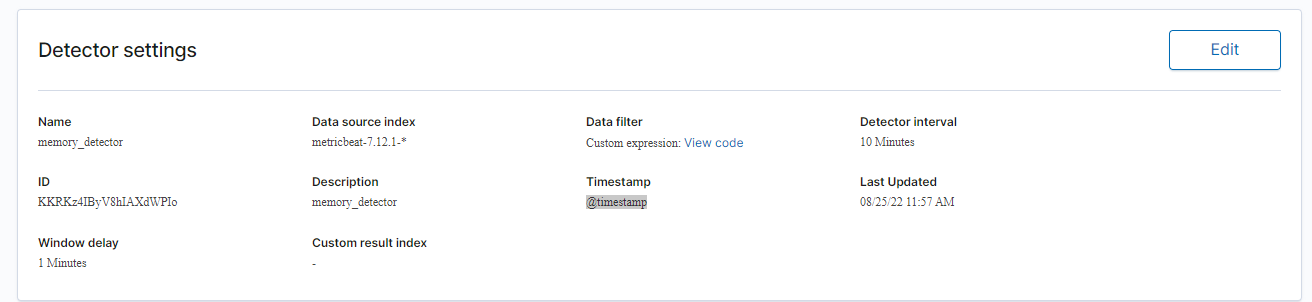


Just remain as usual if you don’t want to change anything. Here we are not using any change.

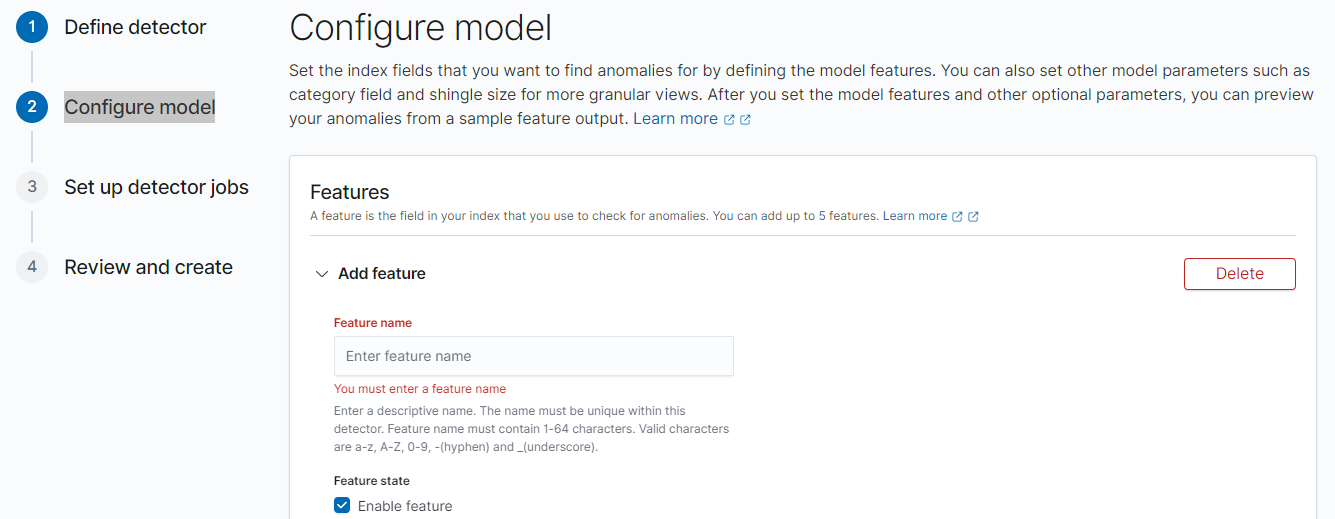
1. Custom result index:



If you want result index then you can mention the name (ex- alert\_index-)



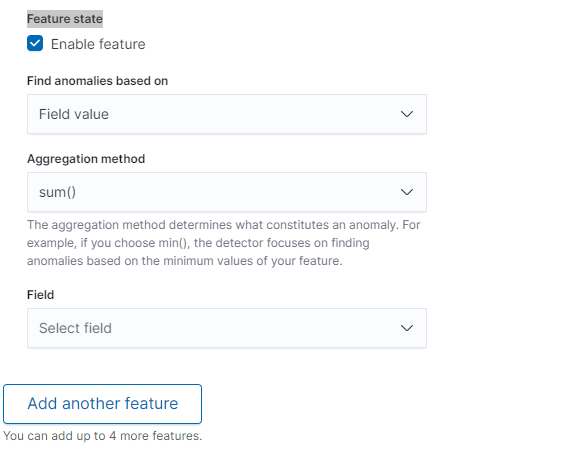
Configure model



1. Feature:

**Feature name-** memory\_detector

1. Feature state:



Field: system.memory.used.pct

Aggregation

method: max

**Feature state-** Enabled

1. Additional settings: