ELK stack

Continuos monitoring

the process used to detect the risk issues associated with an organization operational environment of the application.

So why monitoring through ELK?

What is ELK stack?

collection of 3 opensource products used for monitoring logs from application and system.

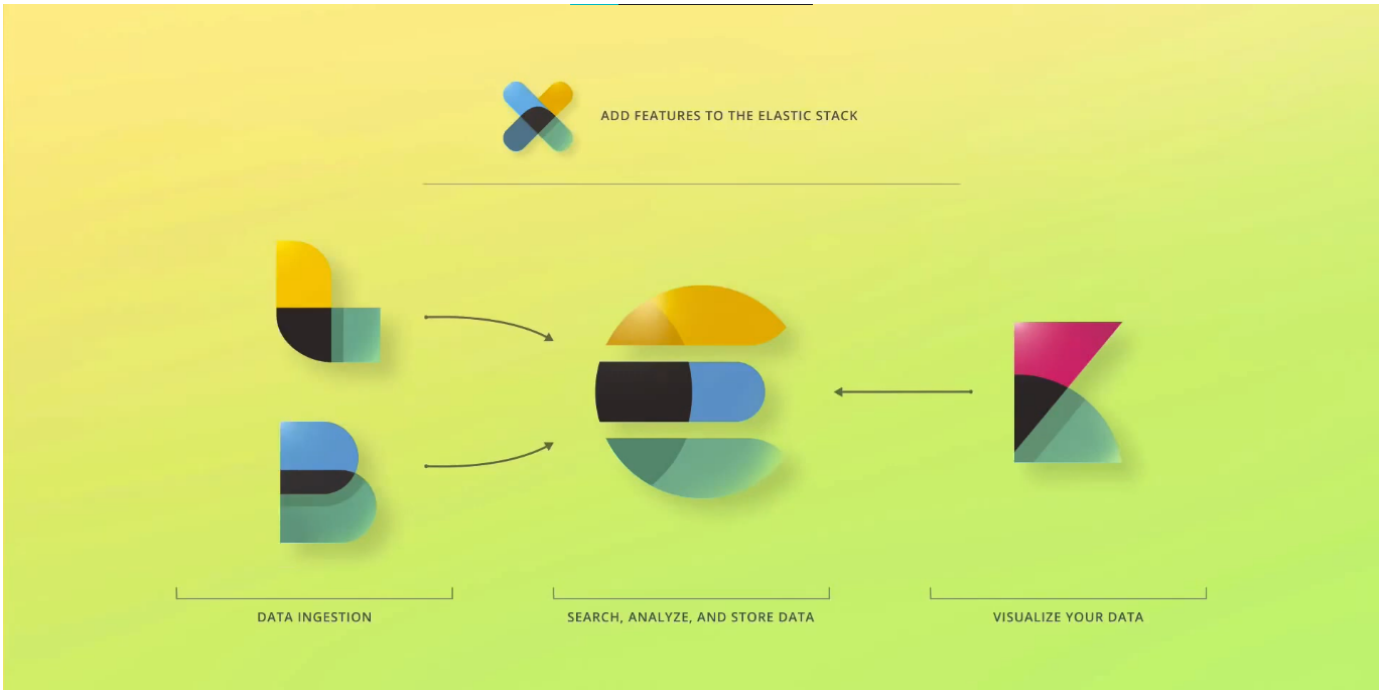
What is Kibana? (An analytics and visualization platform)
The visualization tool for collected data from machine or container. (Graph. Charts)

What is Elastic Search?
Elastic search is a distrubuted, free and open source analytic engine for all type of data.

What is Logstash?
Logstash is a lightweight opensource server side data processing pipeline that allows you to collect data from various sources. (data pipleline for elastic search)

NOTE:: Errors in logs can be searched by SQL queries.

Beats? (Filebeat, metricbeat, packetbeat winlogbeat, auditbeat, heartbeat)



Logstash or beats send data to elastic search in json or xml format.

Elastic search sends stored data to kibana then kibana shows us on dashboard.