## ELK Stack Architecture

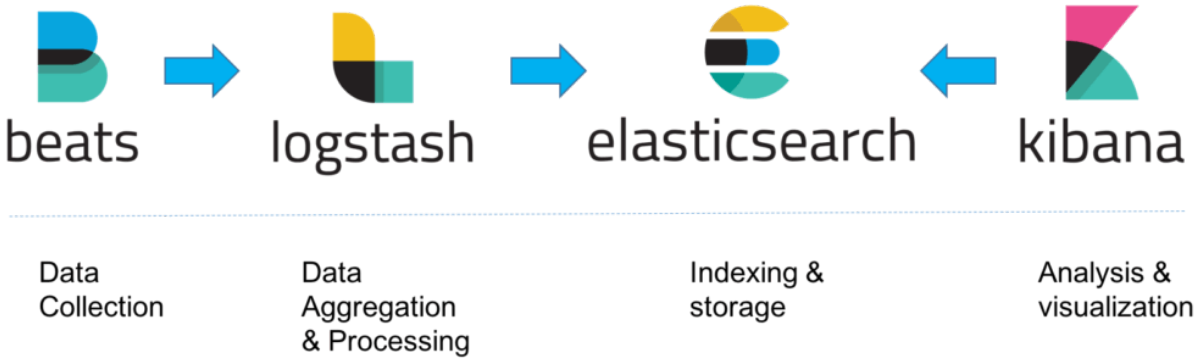
End-to-end log analysis solution


- Logs: Server logs that need to be analyzed
- Logstash: Collect logs and events data. It parses and transforms data
- ElasticSearch: The transformed data from Logstash is Stored and ready to be searched and analyzed
- Kibana: Uses ElasticSearch DB to Explore, Visualize, and Share

One more component was added for Data Collection called Beats. This led Elastic to rename ELK as the Elastic stack.

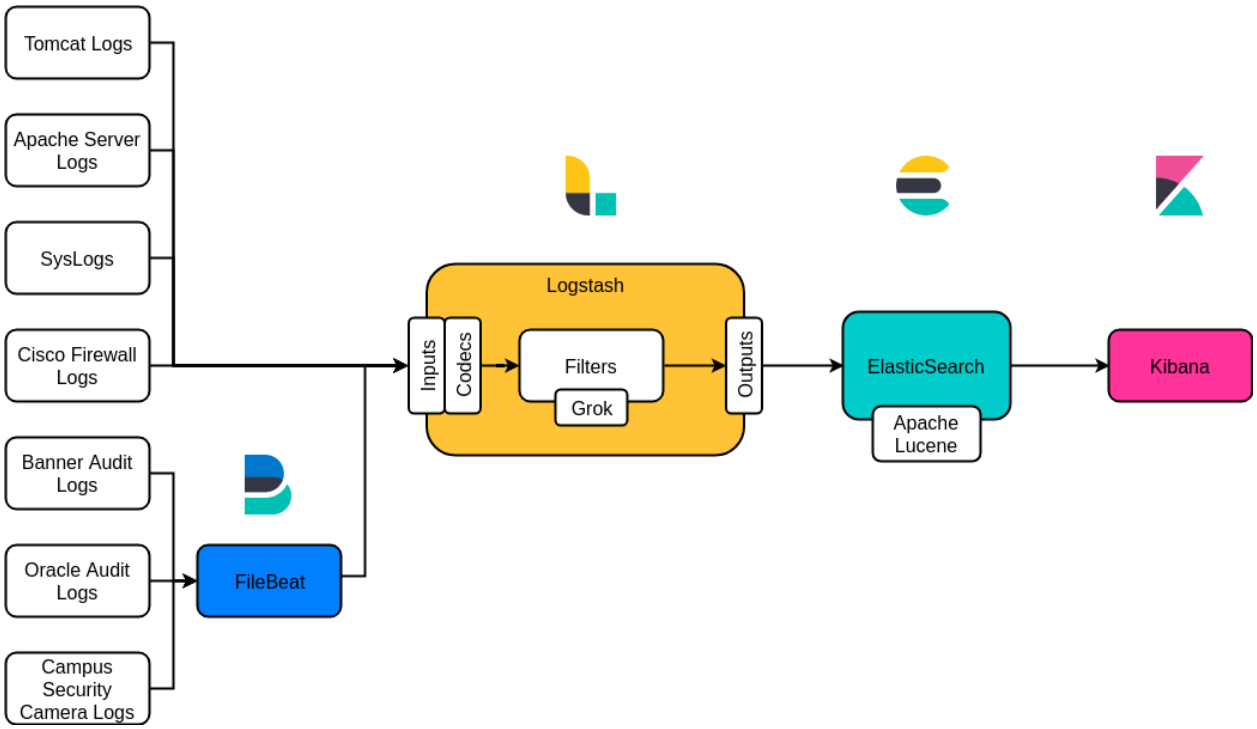
- Beats: Sends data from edge machines to Logstash

## The Elastic Stack




The elastic stack is an end-to-end log analysis solution which helps in deep searching, analyzing, and visualizing the logs generated from different machines.
Log files contain invaluable information that is often unstructured and hard to make sense of and companies will often neglect to analyze their logs. Without careful and detailed analysis of log data organizations can remain oblivious to both opportunities as well as potential threats.

# The Elastic Stack at Snow College




- FileBeat: A lightweight shipper for forwarding and centralizing log data. For each log that Filebeat locates it starts a harvester. Each harvester reads a single log for new content and sends the log data to libbeat, which aggregates the events and send the aggregated data to the output that you've configured for Filebeat.
    - Inputs: An input is responsible for managing the harvesters and finding all sources to read from. If the input type is log, the input finds all files on the drive that match the defined glob paths and starts a new harvester for each file.
    - Harvesters: A harvester is responsible for reading the content of a single file. It reads each file, line by line, and sends the content to the output.