**Getting Started**

* + Overview of the Elastic Stack (ELK+)
  + Introduction to Elasticsearch,Logstash,Kibana
  + Introduction to ELK Stack
  + The birth of Elastic Stack
  + Who uses Elastic Stack?
  + Stack competitors
  + Setting up Elastic Stack

**Analyzing Log Data - Exploring Logstash and Its Plugins**

* + Introduction to Logstash
  + Why do we need Logstash?
  + Features of Logstash
  + Logstash Plugin Architecture
  + Logstash Configuration File Structure
  + Types of Plugins
  + Exploring Input Plugins
  + Exploring Filter Plugins
  + Exploring Output Plugins
  + Logstash command-line options
  + Logstash Configuration for Parsing Logs
  + Execution Model
  + Configure the log file
  + Stash your first event in Logstash
  + Parsing Logs with Logstash
  + Configuring Grok Plugin

**Architecture of Elasticsearch**

* + Nodes & Clusters
  + Indices & Documents
  + Types
  + Sharding
  + Replication
  + Exploring the cluster

### Managing Documents,Mapping

* + Creating an index
  + Adding documents
  + Retrieving documents by ID
  + Replacing documents
  + Updating documents
  + Deleting documents
  + Deleting indices
  + Introduction to mapping
  + Dynamic mapping

### Understaning Inverted Index, Routing

### Analysis & Analyzers

* + Introduction to the analysis process
  + A closer look at analyzers
  + Using the Analyze API
  + Understanding the inverted index
  + Analyzers
  + Overview of character filters
  + Overview of tokenizers
  + Overview of token filters
  + Overview of built-in analyzers

### Introduction to Searching

* + Search methods
  + Searching with the request URI
  + Introducing the Query DSL
  + Understanding query results

### Full Text Queries

* + Introduction to full text queries
  + Term Queries Vs Full text Queries
  + Match
  + Flexible matching with the match query
  + Matching phrases
  + Searching multiple fields
  + Searching Exact Phrases

### Adding Boolean Logic to Queries

* + Introduction to compound queries
  + Querying with boolean logic
  + How the “match” query works

### Controlling Query Results

* + Specifying the result format
  + Source filtering
  + Specifying the result size
  + Specifying an offset

### Analytics with Elasticsearch - Aggregations

* + Introduction to aggregations
  + Metric aggregations
  + Average
  + Sum
  + Extended stats
  + bucket aggregations
  + terms
  + date histogram
  + range

### Visualization with Kibana - Kibana Interface

* + Kibana and its offerings
  + Exploring the discover interface
  + Time Filter
  + Querying and Searching data
  + Fields and filters
  + Discovery page options
  + Creating And Exploring the visualize interface
  + Creating And Exploring the Dashboard interface
  + Exploring Dev Tools
  + Exploring the Management interface
  + Putting it all together

### Best Practices

* + Overview of best practices
  + CPU
  + Memory
  + Nodes Configuration

### Project – Analyzing Apache Webserver Logs ( End to End scenarios covering Logstash, Elastic Search, Kibana Together)

* + We will load dataset containing 50K apache logs using Logstash and transform the data using grok filter. Subsequently, this data will be stored in Elastic Search, we will look at kibana to create dashboards for gaining insights such as top 10 URLs etc ..