Pre-requisites and Important Notes:

- Participants should be comfortable to work with Data Engineering concepts

- Trainer will use sample data for demonstration

- Scope of this training is limited to the topics which are mentioned in this TOC. In case any other related or subtopic to be covered during the training, that needs to be explicitly mentioned in this TOC.

- Sample data available will be used for demonstration and Hands-on

- Trainer will explain the topics via Demonstration. Participants need to do the hands-on post training hours daily. In case the time is available during the training hours then participants are welcome to do the Hands-on as well.

- All the participants need to pre-reed the study material and PPTs before coming to the session for next day.

- Every participant needs to invest at least 2 hours for offline study as well. However, 4 hours is recommended.

- This training will be 70% to 80% on Demonstration by the trainer.

Course Content (40 Hours)

- Getting Started

  o Elastic Stack Overview

  o Elasticsearch Overview

- Installation and Configuration

  o Deploy Elasticsearch

  o Configure and Start a Multi-Node Cluster

  o Deploy Kibana

  o Interface with Elasticsearch in Kibana

- Data Visualization with Kibana

  o Add Sample data to Kibana

  o Creating index patterns

  o Kibana Query Language (KQL)

  o Saving queries

  o Kibana Dashboard

  o Important Metrics to Monitor

- Security

  o Create Your Own PKI

  o Encrypt the Transport Network

  o Set Built-in Passwords

  o Encrypt the Client Network

  o Define Roles

  o Create Users

- Index

  o Define Indices

  o Creating Indices

  o Defining Index Templates

  o Creating Index Templates

- o Using Data Visualizer to Upload Data

- o Bulk Index Data

- o Perform CRUD Operations

- Query

  - o Types of Search Queries?

  - o Execute Non-Analyzed Search Queries

  - o Execute Analyzed Search Queries

  - o Define Metric Aggregations

  - o Define Bucket Aggregations

  - o Define Sub-Aggregations

  - o Searching Data with Term-Level Queries

  - o Searching Data with Full-Text Queries

  - o Compound Search Queries

  - o Combining Queries with Compound Searching

  - o Asynchronous Search Queries

  - o Cross-Cluster Search Queries

  - o Search Across Multiple Clusters

- Aggregating Data

  - o Introduction to Aggregating Data

  - o Writing Metrics Aggregations

  - o Writing Bucket Aggregations

  - o Writing Sub-Aggregations

  - o Performing Metrics and Bucket Aggregations

- Data Processing

  - o Introduction to Data Processing

  - o Explicitly Mapping Fields

  - o Dynamically Mapping Fields

  - o Defining a Custom Analyzer

  - o Defining Multi-Fields

  - o Reindexing Documents

Optional (If time permits):

Establishing an Index Lifecycle Management (ILM) Policy and Managing ILM

Streaming Data in Elasticsearch

- **Developing Search Applications**

  - Introduction

  - Highlighting Search Terms

  - Sorting Search Results

  - Paginating Search Results

  - Redefining Index Aliases

  - Defining Search Templates

  - Developing Search Applications