# Elastic Stack – Course Outline

## 1. Duration

- 48 Hours (6 Days)

## 2. Objectives

At end of this workshop, participants will be able to :

- Understand Elastic Stack architecture and components
- Deploy and configure the stack on-premise as containers
- Ingest, parse, index, search, and visualize data
- Set up alerts/notifications
- Integrate SDKs with applications (Java/Python/.Net)
- Secure the Elastic stack
- Understand limitations for legacy systems
- Size and deploy Elastic APM for monitoring
- Apply real-world telecom-specific use cases
- Build visualizations and dashboards using both Kibana and Grafana

## 3. Audience

Developers, Build/Release Engineers, Quality Engineers, Architects and DevOps professionals

## 4. Pre-requisite

- Basic understanding of logs, applications, system metrics and observability / monitoring
- Basic understanding on Docker containers and compose
- Programming experience in Java, Python, or .NET is helpful

## 5. Hardware & Network Requirements

- Desktop/Laptop with minimum 16 GB RAM
- Open Internet connection (minimum 10 Mbps per user)
- Local Admin Access

## 6. Software Requirements

- Windows / Linux / Mac OS
- Git Client
- Postman
- Java 17+
- Python 3.12+
- .Net SDK 8+
- VS Code IDE (with Java, Python, C# extensions)
- Docker Desktop (latest version)

## 7. Outline

## Day 1

### Module-1: Introduction & Elastic Stack Architecture

- What is Elastic Stack (ELK + Beats + APM)
- Telecom-specific use cases
- CAP Theorem, NoSQL vs RDBMS
- Solr vs Lucene vs Elasticsearch
- Self-hosted deployment architecture (single-node/multi-node)
- Components overview (Elasticsearch, Logstash, Kibana, Beats, APM)

### Module-2 Elasticsearch Setup & Concepts

- Cluster, Node, Index, Shard, Replica
- Install & Configure Elasticsearch (locally/self-hosted)
- Basic cluster health check and configuration
- Hands-on: Install Elasticsearch, create index, insert & retrieve documents

### Module-3 Indexing & Mapping Strategies

- Indexing Overview
- CRUD operations
- Mappings & Data Types
- Dynamic vs Static Mapping
- Data modeling for telecom logs and CDRs

## Day 2

### Module-4: Text Analysis & Tokenization

- Analyzers, Tokenizers, Filters
- Inverted Index, Stemming, Synonyms, N-Gram
- Hands-on: Custom analyzer with sample telecom error logs

### Module-5: Basic to Intermediate Search

- URI Search vs DSL
- Match, Term, Boolean, Fuzzy, Range queries
- Scoring and relevance
- Hands-on: Search queries on telecom event logs

## Day 3

### Module-6: Advanced Search & Aggregations

- Full-text search, Wildcard, Suggesters
- Aggregations: Metric and Bucket types
- Hands-on: Aggregations for call drops, errors, duration buckets

### Module-7: Data Ingestion with Logstash

- Logstash architecture and plugins
- Grok filters, conditionals, mutate, json
- Hands-on: Logstash pipeline for parsing telecom logs

### Module-8: Filebeat for Lightweight Log Shipping

- Filebeat architecture and modules
- Filebeat to Logstash vs Elasticsearch
- Hands-on: Configure Filebeat for sample logs

## Day 4

### Module-9: Data Exploration & Visualization with Kibana

- Index Patterns, Discover, Dev Tools
- Creating visualizations and dashboards
- Hands-on: Build a dashboard with saved visualizations

### Module 10: Visualization with Grafana (New)

- Introduction to Grafana
- Integrating Grafana with Elasticsearch
- Building dashboards in Grafana vs Kibana
- Hands-on: Compare Kibana & Grafana dashboards

### Module-11: Alerting & Monitoring

- Kibana & Watcher alerting (self-hosted)
- Notification: email, Slack, webhook
- Hands-on: Alert on error rate spike

## Day 5

### Module-12: SDK Integration (Java / Python / .Net)

- Java SDK: RestHighLevelClient
- Python SDK: elasticsearch-py
- .NET SDK integration basics
- Hands-on: Java/Python/.Net app integration with Elasticsearch

### Module-13: Elastic APM – Observability & Tracing

- APM architecture and data flow
- Supported language agents: Java, .NET, Python, OpenTelemetry
- Hands-on: Setup APM for Java/Python/.Net apps

### Module-14 Elastic Security

- TLS setup, RBAC, User/Role management
- Hands-on: Secure access to Kibana dashboards

## Day 6

### Module-15: APM Deployment Design

- Sizing guidelines, retention policies
- Deployment topologies for APM

### Module-16: Elastic Stack Limitations for Legacy Apps

- Challenges with unstructured logs
- Compatibility and modeling gaps

### Module-17: Generative AI with Elasticsearch

- Introduction to GenAI with Elastic Stack
- RAG (Retrieval-Augmented Generation) overview
- Elasticsearch as a Vector Database

### Module-18: Case Studies, Best Practices and Emerging Trends

- Usecases and Case Studies
- Elastic Stack Best Practices
- Emerging Trends in Elastic Stack