

ELK Stack – 2 Days (Intermediate Level)

Day 1: Elasticsearch & Logstash Deep Dive

Module 1: ELK Recap & Architecture

- Components refresher: Elasticsearch, Logstash, Kibana, Beats
- ELK vs OpenSearch differences
- Data flow in ELK stack

Module 2: Elasticsearch Core Concepts

- Indexes, documents, and shards
- Mapping & field types (static vs dynamic mapping)
- Analyzers & tokenizers for text search
- Index lifecycle management (ILM)

Module 3: Querying & Aggregations

- Elasticsearch Query DSL basics
- Full-text search vs structured queries
- Aggregations (metrics, bucket, pipeline)
- Filtering vs queries (performance implications)

Module 4: Logstash & Ingest Pipelines

- Logstash pipeline architecture
- Input, filter, output plugins
- Data enrichment with Logstash filters (grok, mutate, date, geoip)
- Elasticsearch ingest pipelines vs Logstash

Day 2: Kibana, Beats & Integrations

Module 5: Kibana for Data Visualization

- Discover, Visualize, Dashboard modules
- Lens visualization
- Kibana Canvas & Reporting
- Security: roles & spaces in Kibana

Module 6: Beats & Data Shipping

- Filebeat, Metricbeat, Packetbeat overview
- Filebeat modules (nginx, apache, system logs)
- Centralized management of Beats

Module 7: Scaling & Performance

- Cluster architecture (nodes, master, data, ingest)
- Index lifecycle & rollover strategy
- Snapshot & restore for backup/recovery
- Monitoring ELK with X-Pack / Metricbeat

Module 8: Integrations & Use Cases

- ELK with DevOps tools (Jenkins, Docker, Kubernetes)
- SIEM & Security use cases (Elastic Security)
- Observability use cases (logs, metrics, traces with Elastic APM)
- ELK vs Splunk vs Datadog