ELASTIC OBSERVABILITY ENGINEER

This two-part, instructor-led course provides a strong foundation on using the Elastic Stack to implement system observability. You will learn how to collect logs, metrics, and APM data, and then ship them to a single datastore — Elasticsearch. You will also learn how unified observability data can be made even more actionable through machine learning and alerting, as well as easier to correlate data across different sources. Using Kibana, you will also explore how to visualize your observability data through an intuitive user interface. After completing this two-part course, you will be well on your way to becoming an Elastic Certified Observability Engineer.

LESSONS - PART 1

All lessons include a hands-on lab.

Observability fundamentals
Understand the fundamentals skills for implementing observability with the Elastic Stack. You will learn how detailed event logs show you whether your systems are operating as smoothly as possible. You will also learn how granular resource usage information gives you important insights on how your infrastructure is running. And you will also learn how application traces give detailed information about performance and errors inside your applications and services. You will then learn how these three sources can be used together for full system observability.

Elasticsearch for time-series data
Elasticsearch plays a central role on dealing with time series data (logs, metrics, APM data). Learn how to use Elasticsearch for managing time series data. Learn the main Elasticsearch concepts such as clusters, nodes, indices, and shards. Briefly explore the different data structures used to store and search data and how to structure your data consistently. Learn how to search and aggregate data as well as how to use index lifecycle management (ILM) to automate how your indices are managed over time.

Continued on next page
ELASTIC OBSERVABILITY ENGINEER

LESSONS - PART 1 (CONTINUED)
All lessons include a hands-on lab.

Shipping metric data
Learn how to configure Metricbeat to ship metric data to Elasticsearch, how to map data and process documents in Elasticsearch, as well as how to handle exceptions along the way.

Shipping log data
Learn how to set up Filebeat to ship data to Elasticsearch. Also learn how to tag data, parse multi-line log entries, and use conditionals to make decisions about what to do with each log line. Finally, understand concepts for building resilient pipelines and troubleshooting Filebeat.

Application performance monitoring (APM)
Elastic APM is an application performance monitoring system built on the Elastic Stack. Understand how to use Elastic APM for monitoring software services and applications in real time. Learn about the different components of Elastic APM and how they work together. You will also learn how to instrument applications to automatically collect detailed performance information with little or no change to your code. You will also learn how Elastic APM supports distributed tracing, as well as how it enables you to analyze performance throughout your microservices architecture all from one UI.

Observability apps
Learn how to monitor the period of time in which a computer service is available with Elastic Uptime. Learn how to use the Metrics app to monitor your infrastructure metrics and identify problems in real time. Learn how to use the Logs app to explore and filter your logs in real time as well as how to customize the output to focus on the data you want to analyze. Learn how to read the performance data that APM agents automatically collect about HTTP requests, database queries, and much more. Also, learn how to find errors in your application with Elastic APM and how to track the error root cause through stack frames.
ELASTIC OBSERVABILITY ENGINEER

LESSONS - PART 2
All lessons include a hands-on lab.

Structuring data
Learn how to structure your unstructured data using Elasticsearch ingest nodes. You will learn how to parse unstructured event data in hybrid cases using split and kv processors as well as dissect and grok patterns. You will also learn how to handle and debug ingest errors along the way.

Processing data
Learn how to use ingest pipelines for converting, enriching and processing your data in any way you want. You will learn how to access document and metadata fields inside processors as well as manipulate them the way you want. You will also learn how to conditionally execute processors.

Kibana for time series
Learn how to leverage Kibana as an observability visualization platform. You will write simple, yet powerful queries to search through your observability data, and combine them with dazzling visualizations. You will also learn how you can use your geographical data to leverage existing query capabilities and build more powerful, interactive, and customizable visualization layers.

Data ingestion architectures
Learn about the different ingestion architectures that you can use, including the use of external tools such as load balancers and distributed message queues. After choosing the adequate architecture, learn how to scale this up and fine tune your ingestion pipeline.

Monitoring the Elastic Stack
Active monitoring makes it easier to be ahead of issues, ensuring your infrastructure is collecting all the data that you expect. Learn how to use the Elastic Stack to monitor itself. Also learn how to collect data from the Elasticsearch nodes, Logstash nodes, Kibana instances, and Beats agents. You will also explore how to visualize your monitoring data from Kibana.

Machine learning and alerting on observability data
Learn how extracting new insights from your observability data is as simple as clicking a button, making machine learning truly operational. Also learn how to use time series modeling to detect anomalies in your current data and forecast trends based on historical data as well as how to configure alerts on top of machine learning to get notified when anomalies are found in your observability data.