

# INTRODUCTION TO ES|QL

In this course, students will develop the skills and knowledge required to build ES|QL pipelines to speed up data analysis and investigation processes. Students will also learn how ES|QL simplifies searching, aggregating, and visualizing large data sets.

## LESSONS

*Includes a hands-on lab.*

### Retrieving and Processing Data - 4 lessons

#### ES|QL quickstart

In this lesson, you will learn ES|QL syntax, how ES|QL queries can be executed, and how results can be interpreted.

#### Retrieving data

In this lesson, you will learn to write ES|QL queries to retrieve and process data from Elasticsearch.

#### Conditions

In this lesson, you will learn to use conditionals, relational operators, and boolean functions in ES|QL.

#### Aggregations

In this lesson, you will learn to use aggregation functions to group and apply metrics to data.

### Exploring Data and Solving Problems - 4 lessons

#### Structuring string data

In this lesson, you will learn about the use of dissect and grok in ES|QL.

#### Enriching data

In this lesson, you will learn more about the enrich processing command to add data from an Elasticsearch index to the output of a query.

#### ES|QL workflow in Kibana

In this lesson, you will learn to use Discover and Lens suggestions to develop a workflow for data exploration and visualization

#### Problem solving with ES|QL

In this lesson, you will learn how to use ES|QL to solve everyday use cases elegantly and efficiently.

## COURSE INFORMATION

### Audience

Developers, Analysts, Administrators, Threat Hunters

### Duration

8 hours

### Language

English

### Prerequisites

- Completion of either **Elasticsearch Engineer** or **Data Analysis with Kibana** is required.
- Completion of both **Elasticsearch Engineer** and **Data Analysis with Kibana** is strongly recommended.

### Requirements

- Stable internet connection
- Mac, Linux, or Windows
- Latest version of Chrome or Firefox (other browsers not supported)
- Disable any ad blockers and restart your browser before class