

One day Training Course: Price £895.00 + VAT per delegate

This follow-on course to the Using Splunk class focuses on Splunk's search and reporting commands. Scenario based examples and hands-on challenges enable users to create robust searches, reports and charts.

Course Topics

- Gain a deeper understanding of search and reporting concepts
- Perform statistical calculations and evaluations on events
- Generate robust reports and charts
- Create and use lookups
- Create and use macros
- Create subsearches
- Understand and use summary indexing

Class Format

Instructor-led lecture with labs. Delivered via virtual classroom or at your site.

Course Objectives

Lesson One – Search Fundamentals

- Examine the anatomy of a search
- Understand search language syntax concepts
- Review fields and use the fields command
- Create a table
- Extract fields
- Examine multi-value fields

Lesson Two – Getting Statistics

- Understand the stats command
- Preview reporting and charting commands
- Display top and rare values for given fields
- Use the stats command to get counts, sums, averages, and field values
- Get summary statistics for a group of events

Lesson Three – Formatting and Calculating

- Understand the eval command
- Perform calculations on values with eval
- Convert, round, and format values
- Use conditional statements
- Further filter calculated results

Lesson Four - Charting

- Identify chart types and the chart command
- Create a chart
- Split values into multiple series
- Define charting modes
- Omit null and other values from charts
- Create a timechart
- Chart multiple values on the same timeline
- Group data with buckets
- Create a rangemap

Lesson Five – Correlating Events

- Identify transactions
- Group events using fields and time
- Search and Report with transactions
- Determine when to use transactions vs stats

Lesson Six – Enriching Data with Lookups

- Understand lookups
- Examine a lookup file example
- Create a lookup table
- Define a lookup
- Configure an automatic lookup
- Use lookups in searches and reports

Lesson Seven – Using Macros

- Understand macros
- Create a basic macro
- Define arguments / variables for a macro
- Use macros in searches

Lesson Eight – Using Subsearches

- Understand subsearches
- Generate a report using a subsearch

Lesson Nine – Summary Indexing

- Define summary indexing
- Create and schedule a summary search
- Run searches against a summary index
- Identify gaps and overlaps in the summary index
- Correct gaps and overlaps in the summary index