splunk>

Splunk Fundamentals 3

The Splunk Fundamentals 3 course picks up where Splunk Fundamentals 2 leaves off, focusing on additional search commands as well as on advanced use of knowledge objects. Major topics include advanced statistics and eval commands, advanced lookup topics, advanced alert actions, using regex and erex to extract fields, using spath to work with self-referencing data, creating nested macros and macros with event types, and accelerating reports and data models.

Course Topics

- Statistical Commands
- eval Commands
- Lookups
- Alert Actions
- Advanced Field Creation and Management
- Working with Self-Describing Data and Files
- Advanced Macros
- Using Acceleration Options

Course Prerequisites

Splunk Fundamentals Part 2

Class Format

Instructor-led lecture with labs, delivered via virtual classroom or at your site

Course Objectives

Module 1 – Exploring Statistical Commands

- Performing statistical analysis with functions of the stat command
- Using fieldsummary
- Using appendpipe
- Using eventstats
- Using streamstats

Module 2 – Exploring eval Command Functions

- Using conversion functions
- Using data and time functions
- Using string functions
- Using comparison and conditional functions
- Using informational functions
- Using statistical functions
- Using mathematical functions
- Using cryptographic functions

Module 3 – Exploring Lookups

- Including and excluding events based on lookup values
- Using KV Store lookups
- Using external lookups
- Using geospatial lookups
- Using database lookups
- Understanding best practices for lookups

Module 4 – Exploring Alerts

- Referencing lookups in alerts
- Outputting alert results to a lookup
- Logging and indexing searchable alert events
- Using a webhook alert action

Module 5 – Advanced Field Creation and Management

- Using regex
- Using the erex command
- Using the rex command
- Identifying regex best practices

Module 6 – Working with Self-Describing Data and Files

- Using the spath command
- Using the eval command with the spath function
- Extracting fields from table-formatted events with multikv

Module 7 – Advanced Search Macros

- Using nested search macros
- Previewing search macros before executing
- Using tags and event types in search macros

Module 8 – Using Acceleration Options: Reports and Summary Indexing

- Using report acceleration
- Using summary indexing

Module 9 – Using Acceleration Options: Data Models and tsidx Files

- Exploring data models using the datamodel command
- Using data model acceleration
- Working with tsidx files using the tstats command

About Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all of Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/goto/education

To contact us, email education_AMER@splunk.com

About Splunk

Splunk is software that indexes, manages and enables you to search data from any application, server or network device in real time.

Visit our website at www.splunk.com to download your own free copy.

Splunk Inc.
250 Brannan
San Francisco, CA 94107
866.GET.SPLUNK
(866.438.7758)
sales@splunk.com
support@splunk.com