splunk>

Splunk Fundamentals 2

This course picks up where Splunk 6.6 Fundamentals Part 1 leaves off, focusing on more advanced searching and reporting commands as well as on the creation of knowledge objects.
Scenario-based examples and hands-on challenges coach you step-by-step through the creation of complex searches, reports, and charts. Major topics include using transforming commands and visualizations, filtering and formatting results, correlating events, creating knowledge objects, using field aliases and calculated fields, creating tags and event types, using macros, creating workflow actions and data models, and normalizing data with the Common Interface Model (CIM).

Course Topics

- Transforming commands and visualization
- Filtering and formatting Results
- Correlating events
- Knowledge objects
- Fields (Field aliases, field extractions, calculated fields)
- Tags and event types
- Macros
- Workflow actions
- Data models
- Splunk Common Information Model (CIM)

Course Prerequisites

Splunk 6.6 Fundamentals Part 1

Class Format

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

Course Objectives

Module 1 – Introduction

- Overview of Buttercup Games Inc.
- Lab environment

Module 2 – Beyond Search Fundamentals

- Search fundamentals review
- Case sensitivity
- Using the job inspector to view search performance

Module 3 – Using Transforming Commands for Visualizations

- Explore data structure requirements
- Explore visualization types
- Create and format charts and timecharts

Module 4 – Using Mapping and Single Value Commands

- The iplocation command
- The geostats command
- The geom command
- The addtotals command

Module 5 –Filtering and Formatting Results

- The eval command
- Using the search and where commands to filter results
- The filnull command

Module 6 – Correlating Events

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

Module 7 – Introduction to Knowledge Objects

- Identify naming conventions
- Review permissions
- Manage knowledge objects

Module 8 – Creating and Managing Fields

- Perform regex field extractions using the Field Extractor (FX)
- Perform delimiter field extractions using the FX

Module 9 – Creating Field Aliases and Calculated Fields

- Describe, create, and use field aliases
- Describe, create and use calculated fields

Module 10 – Creating Tags and Event Types

- Create and use tags
- Describe event types and their uses
- Create an event type

Module 11 – Creating and Using Macros

- Describe macros
- Create and use a basic macro
- Define arguments and variables for a macro
- Add and use arguments with a macro

Module 12 – Creating and Using Workflow Actions

- Describe the function of GET, POST, and Search workflow actions
- Create a GET workflow action
- Create a POST workflow action
- Create a Search workflow action

Module 13 – Creating Data Models

- Describe the relationship between data models and pivot
- Identify data model attributes
- Create a data model
- Use a data model in pivot

Module 14 – Using the Common Information Model (CIM) Add-On

- Describe the Splunk CIM
- List the knowledge objects included with the Splunk CIM Add-On
- Use the CIM Add-On to normalize data

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