splunk>

Splunk Fundamentals 1

This course teaches you how to search and navigate in Splunk to create reports and dashboards, both using Splunk's searching and reporting commands and using the product's interactive Pivot tool. Scenario-based examples and hands-on challenges will enable you to create robust searches, reports, and charts.

Course Topics

- Introduction to Splunk's interface
- Basic searching
- Using fields in searches
- Search fundamentals
- Transforming commands
- Creating reports and dashboards
- Datasets
- The Common Information Model (CIM)
- Creating and using lookups
- Scheduled Reports
- Alerts
- Using Pivot

Course Prerequisites

None

Class Format

eLearning

Course Objectives

Module 1 – Introduction

- How to Use the eLearning Interface
- Overview of Buttercup Games Inc.

Module 2 – What is Splunk?

- Splunk components
- Installing Splunk
- Getting data into Splunk

Module 3 – Introduction to Splunk's User Interface

- Understand the uses of Splunk
- Define Splunk Apps
- Customizing your user settings
- Learn basic navigation in Splunk

Module 4 – Basic Searching

- Run basic searches
- Use autocomplete to help build a search
- Set the time range of a search
- Identify the contents of search results
- Refine searches
- Use the timeline
- Work with events
- Control a search job
- Save search results

Module 5 – Using Fields in Searches

- Understand fields
- Use fields in searches
- Use the fields sidebar

Module 6 – Search Language Fundamentals

- Review basic search commands and general search practices
- Examine the search pipeline
- Specify indexes in searches
- Use autocomplete and syntax highlighting
- Use the following commands to perform searches:
  - tables
  - rename
  - fields
  - dedup
  - sort

Module 7 – Using Basic Transforming Commands

- The top command
- The rare command
- The stats command

Module 8 – Creating Reports and Dashboards

- Save a search as a report
- Edit reports
- Create reports that include visualizations such as charts and tables
- Create a dashboard
- Add a report to a dashboard
- Edit a dashboard

Module 9 – Datasets and the Common Information Model

- Naming conventions
- What are datasets?
- What is the Common Information Model (CMI)?

Module 10 – Creating and Using Lookups

- Describe lookups
- Create a lookup file and create a lookup definition
- Configure an automatic lookup

Module 11 – Creating Scheduled Reports and Alerts

- Describe scheduled reports
- Configure scheduled reports
- Describe alerts
- Create alerts
- View fired alerts

Module 12 - Using Pivot

- Describe Pivot
- Understand the relationship between data models and pivot
- Select a data model object
- Create a pivot report
- Create an instant pivot from a search
- Add a pivot report to a dashboard

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