splunk>

Searching & Reporting with Splunk 6

This nine-hour follow-on 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

- Search Fundamentals
- Transforming Commands
  - Deriving Statistics
  - Creating Visualizations
  - Enriching Visualizations
- Manipulating and Filtering Results
- Correlating Events

Course Prerequisites

- Using Splunk

Class Format

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

Course Objectives

Module 1 – Search Fundamentals

- Review basic search commands and general search practices
- Examine the anatomy of a search
- Use the following commands to perform searches:
  - tables
  - rename
  - fields
  - dedup
  - sort

Module 2 – Transforming Commands, P1: Deriving Statistics

- Use the following commands and their functions:
  - top
  - rare
  - stats

Module 3 – Transforming Commands, P2: Creating Visualizations

- Data structure requirements
- Create and format basic charts
- Create and format timecharts

Module 4 – Transforming Commands, P3: Enriching Visualizations

- Use the following commands and their functions:
  - trendline
  - iplocation
  - geostats
  - geom
  - single values
  - addtotals

Module 5 – Manipulating and Filtering Results

- Use the following commands and their functions:
  - eval
  - filnull
  - search
  - where

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

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