

# splunk™

## Using Splunk

### Quickly learn how to use Splunk

Do you want to become a better Splunker?

This four hour course prepares users to get the most out of searching, navigating, alerting and reporting. It's recommended for anyone in your organization who needs to look at log data - from help desk staff to systems administrators and developers.

#### Course Topics:

- What is Splunk? How you will use it?
- How to access and navigate Splunk's web interface
- Splunk's search language
- Using point and click shortcuts in the web interface
- Capture and share knowledge using tags and other techniques
- Creating event types and tags
- Saving and sharing searches
- Creating reports and alerts
- How to get help

#### Class Format

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

#### Course Objectives

##### Lesson One - Overview

- How can Splunk help you?
- What type of data can Splunk digest?
- What help is available?

##### Lesson Two - Searching

- Identify the sections of the Splunk user interface.
- Navigate among Apps.
- Use the Splunk box to enter search commands.
- Distinguish between Splunk-supplied data and event data.
- Use search results to refine your search.
- Use the timerange selector and timeline to spot trends and narrow search results.
- Identify fields.
- Save a search.
- Define event types and tags.
- Use Splunk search syntax.

##### Lesson Three - Reports and Alerts

- Identify the benefits of using reports.

- Turn a search into a report.
- Put a report in a dashboard.
- Create Alerts.
- List the notification methods for Alerts.

##### Lesson Four - Advanced search syntax

- Define data generator commands and data processing commands.
- Describe the search pipeline.
- List several data processing commands.

#### Splunk Education Tracks

The Using Splunk class is one class in a full education program. The below chart shows how it combines with other classes for different types of users.

**User:** For all day-to-day Splunk users including customer support staff, developers, systems administrators and management.

**Administrator:** For administrators of Splunk. (Administrators of other systems who will just be using Splunk should take the User track.)

**Architect:** For architects who will be designing Splunk deployments, including architects on staff at customer deployments as well as partner professional services personnel.

**Developer:** For developers who will integrate, customize and extend Splunk using its APIs and advanced configuration bundling.

**Sales Engineer:** For Splunk OEM and channel partner sales engineering staff who will be selling Splunk.

**Support Engineer:** For Splunk OEM and channel partner support staff who will be providing first line support for Splunk.

Tracks	Classes					
	Using Splunk	Administering Splunk	Deploying Splunk	Developing with Splunk	Selling Splunk	Supporting Splunk
User	✓					
Administrator	✓	✓				
Architect	✓	✓	✓	✓		
Developer	✓			✓		
Sales Engineer	✓	✓	✓	✓	✓	
Support Engineer	✓	✓	✓	✓		✓

#### About Splunk

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

Visit our website at [www.splunk.com](http://www.splunk.com) to download your own free copy.

Splunk Inc.  
250 Brannan Street  
2nd Floor  
San Francisco, CA  
94107  
866.GET.SPLUNK  
(866.438.7758)  
[sales@splunk.com](mailto:sales@splunk.com)