Course Outline

Splunk Fundamentals 1

Course Summary

Description

In this course you will learn the basics of searching and navigating in Splunk. Using fields, how to get statistics from your data, creating reports, dashboards, lookups and alerts will also be covered. At the completion of this course you should be able to create searches, reports, charts and understand Splunk's datasets features along with the Pivot interface. Material will be delivered via lecture and PowerPoint with demonstrations. Students will work with scenario-based examples in a lab environment in order to gain experience and familiarization with the topics covered.

Objectives

By the end of this course, students will learn:

- Introduction to Splunk
- Learning how to do basic searching within Splunk
- Using fields in searches and search fundamentals
- Learning about transforming commands and visualizations
- Creating reports and dashboards
- Creating and using lookups
- Understanding advanced lookups
- Using alerts and alert actions
- Using acceleration options

Topics

- Defining Splunk and what it does
- Types of data and how Splunk works with data
- Overview of Splunk apps
- Overview of Splunk web and Searching and Reporting app
- Search Architecture
- Running basic searches
- Using autocomplete to help build a search
- Setting the time range of a search
- Identifying the contents of search results
- Using fields in searches
- Search fundamentals (Commands)
- Specifying indexes in searches
- Using autocomplete and syntax highlighting
- Using commands in a search
- Exploring visualization types
- Creating and formatting charts and time charts
- Describing lookups
- Configuring an automatic lookup
- Including and excluding events based on lookup values
- Using KV Store lookups
- Using external lookups
- Using geospatial lookups
- Using database lookups
- Describing alerts
- Creating alerts
- Referencing lookups in alerts
- Outputting alert results to a lookup
- Logging and indexing searchable alert events
- Exploring data models using the datamodel command
- Using data model acceleration
- Working with tsidx files using the tstats command

Splunk Fundamentals 1

Course Summary (cont.)

Audience

This course is designed for Students who would like a better understanding of Splunk and basic Splunk skills.

Duration

Two Days

Course Outline

Course Outline