Course Outline

Fundamentals of Splunk 2

Course Summary

Description

This course continues building on searching and reporting commands with the introduction of additional transforming commands such as the eval command. Other major topics to be covered include filtering and formatting results, correlating events, the creation of knowledge objects, using field aliases and calculated fields, creating tags and event types, creation and use of macros, creating workflow actions and data models, and normalizing data with the Common Information Model (CIM).

Objectives

At the end of this course, students will be able to:

- Beyond Search Fundamentals
- Filtering and formatting results
- Advanced eval Commands
- Advanced Statistical Commands
- Correlating Events
- Introduction to Knowledge Objects
- Fields (field extractions, field aliases, calculated fields)
- Advanced Field Creation and Management
- Tags and Event Types
- Macros
- Workflow Actions
- Working with Self-Destructing Data and Files
- Datasets, Data Models, and Pivot Common Information Model (CIM)
- The Common Information Model (CIM)

Topics

- The eval command
- Using the search and where commands to filter results
- The filnull command
- Using conversion functions
- Using data and time functions
- Using string functions
- Using comparison and conditional functions
- Using informational functions
- Using statistical functions
- Using mathematical functions
- Using cryptographic functions
- Performing statistical analysis with functions of the stat command
- Using fieldsummary
- Using appendpipe
- Using eventstats
- Using streamstats
- 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
- Identify naming conventions
- Review permissions
- Manage knowledge objects
- Describe, create, and use field aliases
- Describe, create and use calculated fields
- Using regex
- Using the erex command
- Using the rex command
- Identifying regex best practices
- Create and use a basic macro
- Define arguments and variables for a macro
- Add and use arguments with a macro
- Using nested search macros

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Course Summary (continued)

- Previewing search macros before executing
- Using tags and event types in search macros
- 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
- Using the spath command
- Using the eval command with the spath function
- Extracting fields from table-formatted events with multikv
- Describe the relationship between data models and pivot
- Identify data model attributes
- Describe pivot
- Create a data model
- Select a data model object
- List the knowledge objects included with the Splunk CIM Add-On
- Use the CIM Add-On to normalize data
- Exploring data models using the datamodel command
- Using data model acceleration
- Working with tsidx files using the tstats command

Audience

Students who would like to continue to build on their Splunk knowledge.

Prerequisites

Splunk Fundamentals 1 or a basic understanding of the Splunk interface, and searches and commands.

Duration

Four days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically