

Splunk Power User Fast Start Training

Splunk Authorized Training · Applied Technology Academy

This Power User "Fast Start" course covers over 60 commands, functions, and knowledge objects to provide users with actionable information about searching best practices and knowledge management. Students will learn how to effectively utilize time in searches, work with different time zones, use transforming commands and eval functions to calculate statistics, compare field values with eval functions and eval expressions, manipulate output, normalize fields and field values, correlate and filter data from multiple sources, and create, manage, and share knowledge objects.

LEVEL Advanced	DURATION 4 Days	EXPERIENCE Basic Splunk Searching and Visualizations	AVERAGE SALARY Varies	LABS No
---------------------------------	----------------------------------	---	--	--------------------------

Course Outline

- **Module 1: Working with Time**
 - Formatting Time
 - Comparing Index Time versus Search Time
 - Using Time Commands
 - Working with Time Zones
- **Module 2: Statistical Processing**
 - What is a Data Series?
 - Transforming Data
 - Manipulating Data with eval
 - Formatting Data
- **Module 3: Comparing Values**
 - Using eval to Compare
 - Filtering with where
- **Module 4: Result Modification**
 - Manipulating Output
 - Modifying Results Sets
 - Managing Missing Data
 - Modifying Field Values
 - Normalizing with eval
- **Module 5: Correlation Analysis**
 - Calculate Co-Occurrence Between Fields
 - Analyze Multiple Datasets

- **Module 6: Intro to Knowledge Objects**
 - What are Knowledge Objects?
 - Knowledge Object Settings
 - Managing Knowledge Objects
- **Module 7: Creating Knowledge Objects**
 - Knowledge Objects and Search-time Operations
 - Creating Event Types
 - Using Event Type Builder
 - Creating Workflow Actions
 - Creating Tags and Aliases
 - Creating Search Macros
- **Module 8: Creating Field Extractions**
 - Using the Field Extractor
 - Creating Regex Field Extractions
 - Creating Delimited Field Extractions
- **Module 9: Data Models**
 - Introducing Data Model Datasets
 - Designing Data Models
 - Creating a Pivot
 - Accelerating Data Models

Intended Audience

- IT professionals responsible for managing or analyzing machine-generated data
- System administrators seeking to monitor and troubleshoot infrastructure
- Security analysts who need to search, correlate, and visualize event data
- Data analysts who want to build dashboards and reports in Splunk
- Anyone preparing for Splunk Power User or Admin certifications
- Users new to Splunk who want a structured introduction to searching and visualization

Prerequisites

- How Splunk works
- How to create basic searching and visualizations

Course Objectives

Participants will:

- Utilize over 60 commands and functions to transform, manipulate, normalize, correlate, and filter data.
- Filter data using time modifiers and time commands, and use formatting functions to accommodate various time formats.
- Calculate statistics using transforming commands and mathematical and statistical eval functions.

Compare, manipulate, and normalize data using several commands, including the all-powerful eval command and an array of statistical, comparison, conditional, and formatting functions.

- Calculate co-occurrence between fields and analyze data from multiple datasets.
- Create, curate, manage, and share knowledge objects.

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.