Working with Time

Course Description:

This course is for Splunk users, analysts, and administrators who want to deepen their understanding of time-based data analysis in Splunk.

This course covers working with time values and using time commads in Splunk. You will learn how to define and adjust time ranges and format timestamps. Key topics include using the time range picker, leveraging the timechart command, understanding _time field properties, and aligning searches across various time zones. At the end of this course, you will know how to use time and time-related commands efficiently to enhance your searches, visualizations, and overall data analysis.

Course Duration:

1 Day

Prerequisites:

To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:

- Intro to Splunk
- Using Fields
- Visualizations

Course Outlines:

Module 1 – Searching with Time

- Understand the _time field and timestamps
- View and interact with the Event Timeline
- Use the earliest and latest time modifiers
- Use the bin command with the _time field

Module 2 – Formatting Time

- Use various date and time eval functions to format time

Module 3 – Using Time Commands

- Use the timechart command
- Use the timewrap command

Module 4 – Working with Timezones

- Understand how time and timezones are represented in your data
- Determine the time zone of your server
- Use strftime to correct timezones in results

Target Audience:

- Users/Analysts
- Administrators
- Engineers