SPLUNK EDUCATION

Course Description

Correlation Analysis

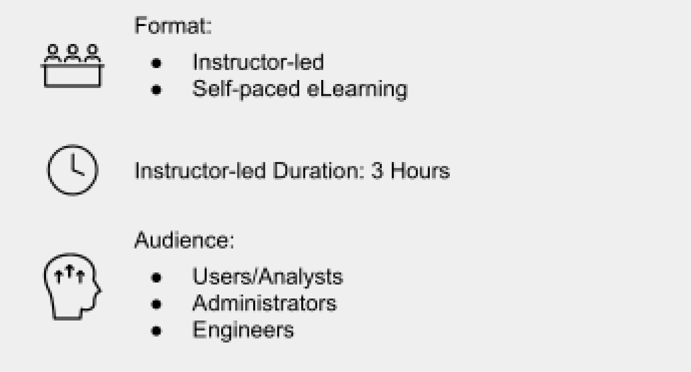
Summary

This course is designed for Splunk power users who want to calculate co-occurrence between fields and analyze data from multiple datasets.

You will learn how to use the transaction, append, appendcols, union, and join commands to correlate events and combine data from various sources.

Prerequisites

- To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:
    - Intro to Splunk
    - Using Fields
    - Visualizations
    - Working with Time
    - Statistical Processing
    - Comparing Values
    - Result Modification
    - Scheduling Reports and Alerts
    - Introduction to Dashboards



Format:

- Instructor-led
- Self-paced eLearning

Instructor-led Duration: 3 Hours

Audience:

- Users/Analysts
- Administrators
- Engineers

Course Outline

Module 1 – Calculate Co-Occurence Between Fields

- Understand transactions
- Explore the transaction command

Module 2 – Analyze Multiple Data Sources

- Understand subsearch
- Use the append, appendcols, union, and join commands to combine, analyze, and compare multiple data sources

About Splunk Education

With Splunk Education, you and your teams can learn to optimize Splunk through self-paced eLearning and instructor-led training, supported by hands-on labs. Explore learning paths and certifications to meet your goals. Splunk courses cover all product areas, supporting specific roles such as Splunk Platform Search Expert, Splunk Enterprise or Cloud Administrator, SOC Analyst or Administrator, DevOps or Site Reliability Engineer, and more. To learn more about our flexible learning options, full course catalog, and Splunk Certification, please visit http://www.splunk.com/education.

To contact us, email education@splunk.com.

splunk> a CISCO company