

Search Under the Hood

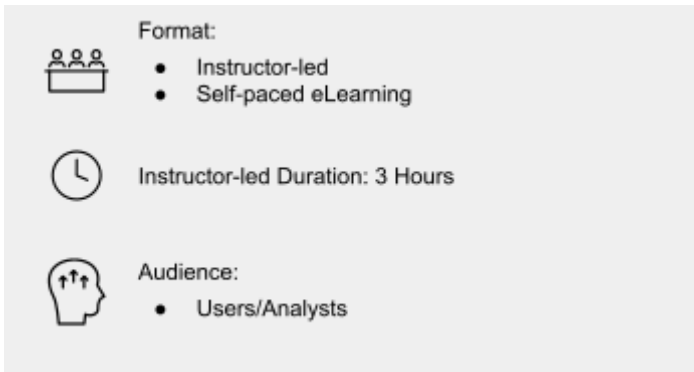
Summary

This course is for students to gain additional insight into how Splunk processes searches.

The course will teach students about Splunk architecture, how components of a search are broken down and distributed across the pipeline, and how to troubleshoot searches when results are not returning as expected.

Prerequisites

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



Format:

- Instructor-led
- Self-paced eLearning

Instructor-led Duration: 3 Hours

Audience:

- Users/Analysts

Course Outline

Module 1 – Investigating Searches

- Use the Search Job Inspector to examine how a search was processed and troubleshoot performance
- Use SPL commenting to help identify and isolate problems

Module 2 – Splunk Architecture

- Understand the role of search heads, indexers, and forwarders in a Splunk deployment
- Understand how the components of a bucket (.tsidx and journal.gz files) are used
- Understand how bloom filters are used to improve search speed

Module 3 – Streaming and Non-Streaming Commands

- Describe the parts of a search string
- Understand the use of centralized vs. distributable commands
- Create more efficient searches

Module 4 – Breakers and Segmentation

- Understand how segmenters are used in Splunk
- Use lippy to reduce the number of events read from disk

Module 5 – Commands and Functions for Troubleshooting

- Using the fieldsummary command
- Using the makeresults command
- Using informational functions with the eval commands
 - the isnull function
 - the typeof function

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.