KIBANA FOR SPLUNK SPL USERS

If you can Splunk, then you can Elastic. This self-paced, on-demand course is designed for users of Splunk’s Search Processing Language (SPL) that would like to translate their analysis skills to Kibana and Elasticsearch. Users will explore the differences and similarities between the two systems, and learn how to easily transition to the Elastic Stack. After completing this course, Splunk SPL users will be able to perform a set of search/query, scripting, and visualization tasks in Kibana.

LESSONS
All lessons include a hands-on lab.

Exploratory analysis
Learn about the fundamental differences in logical containers of data and how targeting datasets for analysis is fundamentally different in Kibana. Learn how to filter data and perform top n analysis (SPL stats and table) in Kibana.

Analysis through visualizations
Understand how charting in Kibana is different from Splunk, and what options are available. Learn how to organize charts and other visualizations in dashboards.

Search time transformations for analysis
Discover the potential of Painless Scripting Language for complex search-time computations. Learn how to implement expressions like eval and replace in Elasticsearch.

COURSE INFORMATION

Audience
Splunk users familiar with Splunk SPL that are interested in migrating to Kibana

Duration
2-3 hours

Language
English

Prerequisites
Familiarity in using Splunk SPL

Requirements
• Stable internet connection
• Mac, Linux, or Windows
• Latest version of Chrome or Firefox (other browsers not supported)
• Disable any ad blockers and restart your browser before class