Course Outline

Splunk User

Course Summary

Objective

After completing this course, students will have a foundational understanding of Splunk software and will be able to perform beginner and intermediate searching, reporting, and dashboarding.

Audience

The “Splunk User” course is targeted for beginner and intermediate users of Splunk;

Topics

- Introduction to Splunk
- Basic Searching
- Using Fields in Search
- Search Language Fundamentals
- Using Basic Transforming Commands
- Creating Reports & Dasboards
- Creating & Using Lookups
- Creating Scheduled Reports & Alerts
- Using Pivot

Prerequisite

There are no prerequisites for this course

Duration

One Day

Course Outline

Splunk User

Course Outline

I. ***Introduction to Splunk***
- A. Describe fundamental Splunk functions such as indexing, searching, enriching data with knowledge, alerting, reporting, and dashboarding.
- B. Cover common use cases for Splunk such as IT operations, Application Development, and IT security.
- C. rovide an overview of the Splunk user interface including navigation menu.

II. ***Basic Searching***
- A. Introduce the main parts of the Search App including search bar, time range picker, “How to Search”, “What to Search”, and “Search History” panels.

III. ***Using Fields in Search***
- A. Understand fields and how to use them in your searches.
- B. Review index time fields including default fields host, source, sourcetype.
- C. Review search time fields and how Splunk extracts fields when you run a search.
- D. Use the fields sidebar to discover automatically extracted fields, view selected and interesting fields, and add fields to your search.
- E. Go over examples for using dynamic field extractor to create custom fields.

IV. ***Search Language Fundamentals***

V. ***Using Basic Transforming Commands***
- A. Understand transforming commands, chart, stats, timechart, top, rare
- B. Review transforming and reporting commands.
- C. Perform Statistical derivations.

VI. ***Creating Reports & Dasboards***
- A. Learn how to create reports with different chart types.
- B. Explore different visualizations available in Splunk.
- C. Learn how to use Dashboard Editor to create, edit dashboard, and format
- D. Visualizations.

VII. ***Creating & Using Lookups***
- A. Learn how to create a lookup file and create a lookup definition.
- B. Review how to configure an automatic lookup.

VIII. ***Creating Scheduled Reports & Alerts***
- A. Learn how to configure scheduled reports.
- B. Walk through creating alerts.

IX. ***Using Pivot***
- A. Walk through an example for using data model builder and Pivot UI.
- B. Use Pivots to search and create reports from a data models.