SPLUNK DEVELOPMENT

Module 1 – Basic Understanding of Architecture

- What are the components
- Discussion on Forwarders- UF/HF
- Common ports for the set up
- License Master/Slave relationship
- Understanding of Deployment Server and Indexer

Module 2 – Introduction to Splunk's User Interface

- Understand the uses of Splunk
- Define Splunk Apps
- Learn basic navigations in Splunk

Module 3 – Searching

- Run basic searches
- Set the time range of a search
- Identify the contents of search results
- Refine searches
- Use the timeline
- Work with events

Control a search job Save search results

Module 4 – Using Fields in Searches

- Understand fields

- Use fields in searches
- Use the fields sidebar

Module 5 – Creating Reports and Visualizations

- Save a search as a report
- Edit reports
- Create reports that include visualizations such as charts and tables
- Add reports to a dashboard

Module 6 – Working with Dashboards

- Creating a dashboard
- Add a reports to a dashboard
- Add a pivot report to a dashboard
- Edit a dashboard

Module 7 – Creating and Managing Alerts

- Describe alerts
- Create alerts
- View fired alerts

Module 8 – Search Fundamentals

- Review basic search commands and general search practices
- Examine the anatomy of a search
- Use the following commands to perform searches:
  - Fields
  - Table
  - Rename
  - Rex
  - Multikv

Module 9 – Reporting Commands, Part 1

- Use the following commands and their functions:

- Top
- Rare
- Stats
- Addcoltals

Module 10 – Reporting Commands, Part 2

- Explore the available visualizations
- Create a basic chart
- Split values into multiple series
- Omit null and other values from chartss
- Create a timechart
- Chart multiple values on the same timeline
- Format charts
- Explain when to use each type of reporting command

Module 11 – Analyzing, Calculating and formatting Results Using the eval command:

- Perform calculations
- Convert values
- Round values
- Format values
- Use conditional statements Further filter calculated results

Module 12 – Creating Field Aliases and Calculated Fields

- Define naming conventions
- Create and use field aliases
- Create and use calculated fields

Module 13 – Creating Tags and Event Types

- Create and use tags

- Describe event types and their uses
- Create an event type

Module 13 – Creating Field Extractions

- Perform field extractions using Field Extractor

Module 14 – Lookups

- Lookups
- Lookup Definition
- Automatic Lookup

Module 15 – Creating and Using Macros

- Describe macros
- Manage macros
- Create and use a basic macro
- Define arguments and variables for a macro
- Add and use arguments with a macro