SPLUNK COURSE CONTENT

Module 1 – Basic Concepts of Splunk Development

- Splunk development concepts
- Roles and responsibilities of Splunk Developer

Module 2 – Saving and Scheduling Searches

- Exporting search results
- Saving and sharing search results
- Saving searches
- Search scheduling

Module 3 – Creating Alerts

- Describing alerts
- Alert Creation
- View fired alerts

Module 4 – Tags and Event Types

- Understanding tags
- Creating tags and using them in a search
- Defining event types and their usefulness
- Creating and using event types in a search

Module 5 – Search Commands

- Reviewing search commands and performing general search practices
- Examine the anatomy of a search
- Using various commands to perform searches:fields, table, rename, rex&erex, multiply

Module 6 – Reporting Commands

- Using following commands and their functions:
- top
- rare
- stats
- addcoltotals
- addtotals

Module 7 – Visualizations

- Explore the available visualizations

- Create Charts and timecharts
- Omit null values and format results

Module 8 – Analyzing, Calculating and Formatting Results

- Using eval command
- Perform calculations
- Value Conversion
- Round values
- Format values
- Conditional statements
- Filtering calculated results

Module 9 – Correlating Events

- Overview of Transactions
- Search Transactions

Module 10 – Enriching Data with Lookups

- What are lookups?
- Lookup file example
- Creating a lookup table
- Defining a lookup
- Configuring an automatic lookup
- Using the lookup in searches and reports

Module 11 – Creating Reports and Dashboards

- Creating reports and charts
- Creating dashboards and adding reports

Module 12 – Getting started with Parsing

- Data Preview and Parsing Phase
- Raw Data Manipulation

Extraction of Fields