Module 1 – Start Searching

Introduce Splunk and the Search app

Run basic searches

Identify the contents of search results

Control a search job

Set the time range of a search

Use the output of a search to refine your search

Module 2 – Saving Results and Searches

Export search results

Save and share search results

Saved searches

Schedule searches

Module 3 – Using Fields

Understand fields

Use fields in searches

Use the fields sidebar

Renaming Fields

Fields Alias

Extracting the fields through IFX

Extracting the fields through regular expressions

Module 4 – Tags and Event Types

Understand tags

Create tags and use tags in a search

Describe event types and their uses

Create and use event types in a search

Module 5 – Creating Alerts

Describe alerts

Create an alert

View fired alerts

Automatically exectuing scripts though alerts

Trouble shooting alerts

Module 6 – Creating Reports

Create reports and charts

Create dashboards and add reports

Create and edit dashboards

Add Visualization to the dashboards

Permission of the dashboard

Conversion of basic XML to advance XML and its usage

Conversion of basic XML to HTML and its usage

Using Inline searches and saved searches in dashboards

Module 7 - Reporting Commands

Using different reporting commands and their functions eg -Top, Rare, Stats, etc

Explore the available visualizations

Create a basic chart

Split values into multiple series

Omit null and other values from charts

Create a timechart

Chart multiple values on the same timeline

Format charts

Explain when to use each type of reporting command

Module 8 - 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 9 - Enriching Data with Lookups

Describe lookups

Examine a lookup file example

Create a lookup table

Define a lookup

Use the lookup in searches and reports