**Splunk Cloud Course Objectives**

**Splunk Cloud**

**Module 1 – Splunk Cloud Overview**

* Describe Cloud topology
* Describe tasks managed by the Splunk cloud administrator
* List the primary differences between Splunk Cloud and Splunk Enterprise
* Environment Setup

**Module 2 – 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 3 – Index Management**

* Define a Splunk Index
* Create indexes in cloud
* Delete data from an index
* Monitor indexing activities

**Module 4 – User Authentication and Authorization**

* Administer Splunk user roles
* New user and role creation
* Assigning capabilities, restrictions and resources to roles.

**Module 5 – Getting Data in**

* List Splunk input options
* Describe the basic settings for an input
* Review Splunk configuration files
* Use a test environment to verify data

**Module 6 – Getting Data in Cloud**

* List Splunk forwarder types
* Describe the role of forwarders
* Configure a forwarder to Splunk Cloud
* Test the forwarder connection
* Describe optional forwarder settings

**Module 7 – Monitor Inputs**

* Describe the Splunk process for inputting data
* Create file and directory monitor inputs
* Use optional settings for monitor inputs

**Module 8 – Fine-tuning Inputs**

* Describe the default processing that occurs during the input phase
* Configure input phase options, such as sourcetype fine-tuning and character set encoding

**Module 9 – Manipulating Raw Data**

* Explain how data transformations are defined and invoked
* Use transformations with props.conf and transforms.conf to modify raw data
* Use SECCMD to modify raw data

**Module 10 – Data Parsing and Filtering**

* Describe the default processing that occurs during parsing
* Optimize and configure event line breaking
* Multiple functionalities of props.conf and transforms.conf
* Explain how timestamps and time zones are extracted or assigned to events
* Use Data Preview to validate event creation during the parsing phase

**Module 11 – Installing and Managing Apps**

* Describe self-service app installs vs. manual app installs
* Provide steps to install apps
* Describe how apps are managed

**Module 12 – Working with Splunk Cloud Support**

* Troubleshooting Splunk deployments
* Collecting data and use diagnostics or monitoring to investigate
* Explore diagnostic tools used to troubleshoot common issues
* Overview of how to submit request with the relevant data for support to troubleshoot

**Module 13 – Forwarder Management**

* Describe Splunk Deployment Server
* Explain the use of forwarder management
* Configure forwarders to be deployment clients
* Managing forwarders using deployment apps

**Module 14 - Cloud Monitoring Console**

* Overview of Cloud Monitoring Console
* License usage
* Indexing overview
* Forwarder management

**Splunk Development**

**Module 15 – Introduction to Splunk's User Interface**

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

**Module 16 – 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 17 – Using Fields in Searches**

* Understand fields
* Use fields in searches
* Use the fields sidebar

**Module 18 – 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 19 – Working with Dashboards**

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

**Module 20 – 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 21 – Reporting Commands, Part 1**

* Use the following commands and their functions:
* Top
* Rare
* Stats
* Addcoltotals

**Module 22 – Reporting Commands, Part 2**

* 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 23 – 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 24 – Creating Field Aliases and Calculated Fields**

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

**Module 25 – Creating Field Extractions**

* Perform field extractions using Field Extractor

**Module 26 – Creating Tags and Event Types**

* Create and use tags
* Describe event types and their uses
* Create an event type

**Module 27 – Creating Workflow Actions**

* Describe the function of a workflow action
* Crate a GET workflow action
* Crate a POST workflow action
* Create a Search workflow action

**Module 28 – Creating and Managing Alerts**

* Describe alerts
* Create alerts
* View fired alerts

**Module 29 – 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