**SPLUNK ADMINISTRATION**

**Module 1 – Introduction to Administration**

* Splunk overview
* Identify Splunk administrator role

**Module 2 – Configuring Forwarders**

* Understand the role of production Indexers and Forwarders
* Understand the functionality of Universal Forwarders and Heavy Forwarders
* Configure Forwarders
* Identify additional Forwarder options

**Module 3 – Monitor Inputs**

* Create file and directory monitor inputs
* Use optional settings for monitor inputs

**Module 4 – Parsing Phase and Data**

* Understand the default processing that occurs during parsing
* Optimize and configure event line breaking

**Module 5 – Manipulating Raw Data**

* Explain how data transformations are defined and invoked
* Use transformations with props.conf and transforms.conf to:
  1. Mask or delete raw data as it is being indexed Override sourcetype or host based upon event values
* Route events to specific indexes based on event content
* Prevent unwanted events from being indexed
* Use SEDCMD to modify raw data

**Module 6 – License Management**

* Identify license types
* Describe license violations
* Add and remove licenses

**Module 7 – Splunk Apps**

* Describe Splunk apps and add-ons
* Install an app on a Splunk instance
* Manage app accessibility and permissions

**Module 8 – Splunk Configuration Files**

* Describe Splunk configuration directory structure
* Understand configuration layering process

**Module 9 – Splunk Indexes**

* Describe index structure
* List types of index buckets
* Create new indexes

**Module 10 – Deleting And Backing Up Data**

* Apply a data retention policy
* Backup data on indexers
* Delete data from an index
* Restore frozen data

**Module 11 – Splunk User Management**

* Describe user roles in Splunk
* Create a custom role
* Add Splunk users

**Module 12 – Deployment Server**

* Set up Deployment Server
* Set up Deployment Client
* Create app
* Create ServerClass
* Deploy apps in the Splunk Environment