



## **Module 1 – Splunk Developer Overview**

- Splunk overview
- Identify Splunk components
- Identify Splunk system administrator role

## **Module 2 – License Management**

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

## **Module 3 – Splunk Apps**

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

## **Module 4 – Splunk Configuration Files**

- Describe Splunk configuration directory structure
- Understand configuration layering process
- Use btool to examine configuration settings

## **Module 5 – Splunk Indexes**

- Describe index structure
- List types of index buckets
- Create new indexes
- Monitor indexes with Monitoring Console



## **Module 6 – Deleting And Backing Up Data**

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

## **Module 7 – Splunk User Management**

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

## **Module 8 – Getting Data In**

- Describe the basic settings for an input
- List Splunk forwarder types
- Configure the forwarder
- Add an input to UF using CLI

## **Module 9 – Distributed Search**

- Describe how distributed search works
- Explain the roles of the search head and search peers
- Configure a distributed search group
- List search head scaling options