Splunk power user TOC (5Full Day)

Day 1: Introduction and Basic Search

1. Introduction to Splunk

- Overview of Splunk
- Splunk Architecture
- Splunk Use Cases

2. Getting Started with Splunk

- Navigating the Splunk Interface
- Basic Splunk Terminology
- Setting Up a Splunk Environment

3. Basic Searching

- Using the Search Bar
- Understanding Search Results
- Search Commands: search, table, fields, rename, dedup, sort

4. Using Time in Searches

- Time Range Picker
- Modifying Time Ranges
- Using Time Modifiers in Searches

5. Saving and Sharing Search Results

- Saving Searches
- Creating Reports
- Sharing Search Results

Day 2: Advanced Search Techniques

1. Search Language Fundamentals

- Search Processing Language (SPL) Basics
- Using Pipes in Searches
- Subsearches

2. Advance Commands

- stats
- chart
- timechart
- eval
- Top / Rare
- Append / Appendcols / Appendpipe
- Join
- Transaction Command
- Tstats

3. Data Visualization

- Creating Charts and Graphs
- Using Visualization Options
- Customizing Dashboards

4. Advanced Search Techniques

- Field Extraction
- Using Lookups
- Combining Searches

5. Working with Alerts

- Setting Up Alerts
- Managing Alerts
- Alert Actions – Triggered Alert, webhook, lookup and logging event in index

6. Workflow Actions

- Creating workflow action
- Event action and field menu creating
- Search type and link type workflow creations

Day 3: Data Management

1. Data Input and Indexing

- Adding Data to Splunk
- Understanding Indexes
- Managing Indexes

2. Field Extraction and Data Normalization

- Automatic vs. Manual Field Extraction
- Rex, erex and Regex Commands
- Field Aliases
- Data Models and Pivots

3. Using Lookups

- Creating and Managing Lookups
- Using Lookups in Searches
- KV Store Lookups

4. Data Enrichment

- Adding Context to Data
- Using Enrichments in Searches
- Data Model Acceleration

5. Managing Knowledge Objects

- Overview of Knowledge Objects
- Creating and Managing Field Extractions
- Managing Tags and Event Types

Day 4: Splunk Visualization and Reporting

1. Creating Dashboards

- Dashboard Overview
- Simple vs. Dynamic Dashboards
- Creating and Editing Dashboards

2. Using Panels and Inputs

- Adding Panels to Dashboards
- Using Inputs for Interactive Dashboards
- Setting Panel Properties

3. Advanced Dashboard Techniques

- Using Tokens and Global Variables
- Drilldowns and Dynamic Actions
- Customising Dashboard Layout

4. Reporting

- Creating Scheduled Reports
- Managing Report Acceleration
- Distributing Reports

5. Splunk Apps and Add-ons

- Installing and Managing Apps
- Popular Splunk Apps for Power Users
- Customizing and Extending Splunk Functionality

Day 5: Performance Tuning and Best Practices

1. Search Optimization

- Optimizing Search Performance
- Using Summary Indexing
- Search Job Management

2. Data Management Best Practices

- Data Retention Policies
- Archiving and Deleting Data
- Managing Disk Space

3. Security and Access Control

- User Roles and Permissions
- Securing Splunk Data
- Monitoring Splunk Activity

4. Troubleshooting and Support

- Common Issues and Solutions
- Using Splunk Support Resources
- Community and Online Resources

5. Final Review and Exam Preparation

- Reviewing Key Concepts
- Practice Exercises and Mock Exams
- Tips for the Splunk Power User Certification Exam