Splunk Certified Power User: 5-Full-Day Training Program

Day 1: Introduction to Splunk and Data Onboarding

1. Overview of Splunk
• What is Splunk?
• Use Cases and Benefits
• Key Components of Splunk: Indexer, Search Head, Forwarders
• Splunk Terminologies

2. Navigating the Splunk Interface
• Splunk Web Overview
• Apps and Dashboards
• Search Bar and Time Picker
• Menu Options

3. Data Onboarding Basics
• Adding Data to Splunk
• File and Directory Monitoring
• Data Inputs Overview (TCP/UDP, REST API, etc.)
• Source Types and Parsing

4. Lab Exercises
• Add a sample data file to Splunk
• Explore the Splunk Web interface

Day 2: Search Fundamentals

1. Search Processing Language (SPL) Basics
• Anatomy of a Search
• Using Fields, Time Ranges, and the Search Pipeline

2. Filtering and Formatting Data
• Using Search Commands: search, fields, rename, table
• Applying Filters: Time and Event Filters

3. Statistical Commands
• Introduction to Stats: stats, chart, timechart
• Aggregation Functions: sum, avg, count, distinct_count

4. Lab Exercises
• Run basic searches and apply filters
• Use stats to summarize data

Day 3: Advanced Searching and Reporting

1. Data Enrichment with Lookups
• Overview of Lookups
• Creating and Configuring Lookups
• Using Lookups in Searches

2. Advanced Search Techniques
• Subsearches
• Joins and Union Searches
• Using Wildcards

3. Reporting and Visualization
• Creating Tables and Charts
• Customizing Dashboards: Panel Configurations and Visualizations
• Exporting and Scheduling Reports

4. Lab Exercises
• Create a lookup and use it in a search
• Build a basic dashboard with interactive panels

Day 4: Alerts, Knowledge Objects, and Data Models

1. Knowledge Objects in Splunk
• Overview: Fields, Event Types, Tags, and Aliases
• Managing Field Extractions
• Working with Saved Searches

2. Alerts and Actions
• Configuring Alerts
• Triggering Conditions
• Scheduling Alerts and Notifications

3. Data Models and Pivot
• Introduction to Data Models
• Creating and Using Data Models
• Working with Pivot

4. Lab Exercises
• Create and test a custom alert
• Build and explore a data model

Day 5: Real-World Use Cases and Exam Preparation

1. Splunk Best Practices
• Efficient Searching Techniques
• Optimizing Performance
• Managing Resources

2. Real-World Use Cases
• Analyzing Logs (System/Application Logs)
• Security Monitoring with Splunk
• Operational Intelligence

3. Splunk Certification Exam Preparation
• Review Key Topics: Search Commands, Dashboards, Alerts, Lookups
• Sample Questions and Mock Exam
• Time Management Tips for the Exam