Technology Name – Splunk Certified Power User

Course Content:
Duration: 5 days

Day 1: Introduction to Splunk and Data Onboarding
Overview of Splunk

- What is Splunk?
- Use Cases and Benefits
- Key Components of Splunk: Indexer, Search Head, Forwarders
- Splunk Terminologies

Navigating the Splunk Interface

- Splunk Web Overview
- Apps and Dashboards
- Search Bar and Time Picker
- Menu Options

Data Onboarding Basics

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

Lab Exercises

- Add a sample data file to Splunk
- Explore the Splunk Web interface

Day 2: Search Fundamentals
Search Processing Language (SPL) Basics

- Anatomy of a Search
- Using Fields, Time Ranges, and the Search Pipeline

Filtering and Formatting Data

- Using Search Commands: search, fields, rename, table
- Applying Filters: Time and Event Filters

Statistical Commands

- Introduction to Stats: stats, chart, timechart
- Aggregation Functions: sum, avg, count, distinct_count

Lab Exercises

- Run basic searches and apply filters
- Use stats to summarize data

Day 3: Advanced Searching and Reporting
Data Enrichment with Lookups

- Overview of Lookups

- Creating and Configuring Lookups
- Using Lookups in Searches

Advanced Search Techniques

- Subsearches
- Joins and Union Searches
- Using Wildcards

Reporting and Visualization

- Creating Tables and Charts
- Customizing Dashboards: Panel Configurations and Visualizations
- Exporting and Scheduling Reports

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

Knowledge Objects in Splunk

- Overview: Fields, Event Types, Tags, and Aliases
- Managing Field Extractions
- Working with Saved Searches

Alerts and Actions

- Configuring Alerts
- Triggering Conditions
- Scheduling Alerts and Notifications

Data Models and Pivot

- Introduction to Data Models
- Creating and Using Data Models
- Working with Pivot

Lab Exercises

- Create and test a custom alert
- Build and explore a data model

Day 5: Real-World Use Cases and Exam Preparation

Splunk Best Practices

- Efficient Searching Techniques
- Optimizing Performance
- Managing Resources

Real-World Use Cases

- Analyzing Logs (System/Application Logs)
- Security Monitoring with Splunk
- Operational Intelligence

Splunk Certification Exam Preparation

- Review Key Topics: Search Commands, Dashboards, Alerts, Lookups
- Sample Questions and Mock Exam
- Time Management Tips for the Exam