

## 5-Day Detailed Training Program: Splunk Certified Core User

### **DAY 1 — INTRODUCTION, DATA INGESTION & SEARCHING**

#### Module 1: Introduction to Splunk (Theory + Hands-on)

- What is Splunk? Why Splunk?
- Splunk Architecture (Indexer, Search Head, Forwarders, DS, HFs)
- Data onboarding lifecycle
- Splunk Web, CLI, REST — Overview
- Lab: Explore Splunk Web, search app, and sample datasets

#### Module 2: Understanding the Splunk Processing Pipeline (Theory)

- Input → Parsing → Indexing → Search
- Line breaking & timestamp extraction
- License usage basics
- Buckets, hot-warm-cold-frozen
- Data retention concepts

#### Module 3: Forwarders & Data Inputs (Theory + Hands-on)

- Types of forwarders: UF vs HF
- Splunk UF installation flow
- Monitoring files, directories, network ports
- Using Inputs.conf
- Lab: Onboard log files using UF & verify indexing

#### Module 4: Basic Searching in Splunk (Theory + Hands-on)

- SPL Overview
- Search pipeline & commands
- Fields, events, timestamps, sourcetype
- Using search modes (Fast / Smart / Verbose)
- Search best practices
- Lab: Basic search using sample logs

### **DAY 2 — SPL COMMANDS, FILTERING, AND FIELD EXTRACTION**

#### Module 5: Filtering, Formatting & Transforming Commands (Hands-on Heavy)

- stats, timechart, table, dedup, sort, where, rename
- Lab: Create reports using stats, timechart, dedup

#### Module 6: Comparison, Boolean & Wildcards (Theory + Hands-on)

- Wildcards, IN, LIKE
- Boolean logic
- Field comparisons
- NULL handling
- Optimizing searches
- Lab: Write complex SPL queries with filters

#### Module 7: Field Discovery & Extraction (Theory + Hands-on)

- Automatic field extraction
- Field extractor tool (FX)
- Regex-based field extraction
- Fields from JSON, XML
- Using eval to create new fields
- Lab: Create regex extractions & validate

#### Module 8: Stats Functions Deep Dive (Hands-on)

- count, avg, sum, values, list, distinct count
- eventstats vs streamstats
- Lab: Build SPL reports using eventstats & streamstats

### DAY 3 — ADVANCED EVAL, LOOKUPS, DATA MODELS & KNOWLEDGE OBJECTS

#### Module 9: Advanced Eval (Hands-on Heavy)

- Conditional eval (if, case)
- String & math functions
- coalesce, replace, substr, split
- Lab: Build computed fields for dashboards

#### Module 10: Lookup Files & KV Store Lookups (Theory + Hands-on)

- CSV lookups
- Automatic lookups
- External lookups
- Troubleshooting lookups
- Lab: Add a CSV lookup for enrichment & create auto-lookup

#### Module 11: Macros, Event Types & Tags (Theory + Hands-on)

- Creating macros
- Event types
- Tagging data
- Lab: Build macro-based search optimization

#### Module 12: Data Models & Pivot (Theory + Hands-on)

- Data model acceleration
- Pivot UI
- When to use Pivot?
- Lab: Create a data model & pivot report

## **DAY 4 — REPORTS, ALERTS, DASHBOARDS & VISUALIZATION TECHNIQUES**

### **Module 13: Creating Reports (Hands-on Heavy)**

- Save search as report
- Scheduled reports
- Export options
- Permissions
- Lab: Create scheduled reports

### **Module 14: Alerts (Theory + Hands-on)**

- Scheduled vs Real-time alerts
- Trigger conditions
- Throttling
- Alert actions (email, webhook)
- Permissions & sharing
- Lab: Create alerts with throttling

### **Module 15: Dashboards (Hands-on Heavy)**

- Dashboard Studio vs Classic
- Panels, charts, tables, maps
- Tokens, Drilldown
- Dashboard best practices
- Lab: Build a Studio dashboard with drilldowns

### **Module 16: Knowledge Management & Apps**

- Splunk roles
- Shared objects
- Splunkbase overview
- Useful apps

## **DAY 5 — USE CASE, EXAM PREP & SCENARIO-BASED LABS**

### **Module 17: End-to-End Use Case (Hands-on Heavy)**

- Upload data → extract fields → dashboards → alerting
- Lab: Full real-world implementation

## <sup>1</sup>Module 18: Optimizing SPL — Search Best Practices

- Tstats, indexed fields, metadata
- Job inspector
- Performance tuning

## Module 19: Scenario-Based Challenges (Hands-on)

- Field extraction challenges
- Dashboard drilldowns
- Filtering & lookup scenarios

## Module 20: Exam Preparation

- Exam format & mock questions
- Tips & strategy
- Revision