# 3-Day Splunk Training

Day 1: Fundamentals
Days 2-3: Administration

# Contents

# 1 Day 1: Splunk Fundamentals

## 1.1 Morning Session (09:30-12:30)

- **Introduction to Splunk (09:30-10:30)**
  - Architecture overview
  - Use cases and applications
  - Hands-on: Accessing Splunk Web
- **Basic Searching (10:30-11:30)**
  - Search Processing Language (SPL) basics
  - Time modifiers and field searching
  - Lab: `index=main | head 100`
- **Field Extraction (11:30-12:30)**
  - Automatic vs manual extraction
  - Using field extractor
  - Lab: Extract fields from sample logs

## 1.2 Afternoon Session (13:30-17:30)

- **Statistical Commands (13:30-15:00)**
  - `stats`, `chart`, `timechart`
  - Aggregation functions
  - Lab: Create request count visualization
- **Alerts & Dashboards (15:00-16:30)**
  - Alert thresholds and actions
  - Dashboard creation
  - Lab: Build CPU usage dashboard
- **Capstone Project (16:30-17:30)**
  - Analyze sample web traffic
  - Present findings in dashboard

# 2 Day 2: Splunk Administration I

## 2.1 Morning Session (09:30-12:30)

- **Installation & Configuration (09:30-10:30)**
  - System requirements
  - Directory structure
  - Lab: Install Splunk Enterprise
- **Index Management (10:30-11:30)**
  - Creating and managing indexes lifecycle management
  - Lab: Create custom index
- **Data Inputs (11:30-12:30)**
  - Forwarder types
  - Network inputs
  - Lab: Configure file monitor

### 2.2 Afternoon Session (13:30-17:30)

- **User Management (13:30-15:00)**
  - Role-based access control
  - Authentication methods
  - Lab: Create custom roles
- **License Management (15:00-16:30)**
  - License types
  - Usage monitoring
  - Lab: Add trial license
- **Admin Lab (16:30-17:30)**
  - Complete system setup
  - Troubleshooting exercise

## 3 Day 3: Splunk Administration II

### 3.1 Morning Session (09:30-12:30)

- **Universal Forwarders (09:30-10:30)**
  - Deployment methods
  - Configuration files
  - Lab: Install and configure UF
- **Deployment Server (10:30-11:30)**
  - Server configuration
  - App deployment
  - Lab: Deploy sample app
- **Configuration Files (11:30-12:30)**
  - inputs.conf, outputs.conf
  - props.conf, transforms.conf
  - Lab: Custom log parsing

### 3.2 Afternoon Session (13:30-17:30)

- **Monitoring & Troubleshooting (13:30-15:00)**
  - Monitoring console
  - Log analysis
  - Lab: Diagnose forwarder issue
- **Best Practices (15:00-16:30)**
  - Performance tuning
  - Security hardening
  - Lab: Optimize search
- **Final Project (16:30-17:30)**
  - End-to-end deployment
  - Knowledge check

## Lab Requirements

| Component | Specification |
|---|---|
| Splunk Enterprise | Version 9.0+ |
| Virtual Machines | 4+ cores, 8GB RAM |
| Sample Data | Apache, Windows Event, Syslog |