

# SPLUNK – User and Administrator

Advance your skills and expertise in a most advanced analytics and event management tool

## Course Brochure and Outline

**CODEC Networks Pvt Ltd**

507, New Delhi House, Barakhamba Road,  
New Delhi 110001

[trainings@codecnetworks.com](mailto:trainings@codecnetworks.com)

+91 11 43752299, 9971676124

## Course Overview

This Splunk User and Admin Training includes concepts which are required for both Splunk Users and Splunk Administrators. By the end of this training, you will learn their roles, responsibilities and be ready for implementation.

This training includes various aspects of Splunk installation, configuration, Syslog Server, log analysis, Splunk dashboard, installation, configuration of Splunk, deploying Splunk search, monitor, index, report and analysis.

Splunk User (Developer) training teaches you how to search and navigate in Splunk, use fields, get statistics from your data, create reports, dashboards, lookups, and alerts. Scenario-based examples and hands-on challenges will enable you to create robust searches, reports, and charts. It will also introduce you to Splunk's datasets features and Pivot interface.

Splunk Data Administrators training teaches you how to getting data into Splunk Indexers. The course provides the knowledge of Splunk forwarders and methods to get remote data into Splunk indexers. It covers installation, configuration, management, monitoring, and troubleshooting of Splunk forwarders and Splunk Deployment Server components.

Splunk System Administrators teaches you how to manage Splunk Enterprise environment. The course provides the knowledge of Splunk license manager, indexers and search heads. It covers configuration, management, and monitoring core Splunk Enterprise components.

After completing of this training program, you should be able to:

- Understand Splunk Power User/ Admin concepts
- Apply various Splunk techniques to visualize data using different graphs and dashboards
- Implement Splunk in the organization to Analyze and Monitor systems for operational intelligence
- Configure alerts and reports for monitoring purposes
- Troubleshoot different application logs issues using SPL (Search Processing Language)
- Implement Splunk Indexers, Search Heads, Forwarder, Deployment Servers & Deployers

## Who Should Attend

The training program is ideal for those working in positions such as, but not limited to -

- IT Operations, IT Monitoring, IT Support, & Data Center teams.
- Data Analysts who want to gain knowledge of Splunk development for creating Apps and Dashboards

## Course Duration

40 Hours (5 Days \* 8 Hours)

## **Course Content / Outline**

### **User (Development) Training (1 Days \* 8 Hours)**

Module 1 - Introduction to Splunk's interface  
Module 2 - Basic searching  
Module 3 - Using fields in searches  
Module 4 - Search fundamentals  
Module 5 - Transforming commands  
Module 6 - Creating reports and dashboards

Module 7 - Datasets  
Module 8- Creating and using lookups  
Module 9 - Scheduled Reports  
Module 10 - Alerts  
Module 11 - Using Pivot

### **Data and System Administration Training (4 Days \* 8 Hours)**

Module 1 - Introduction to Data administration  
Module 2 - Getting Data in-staging  
Module 3 - Forwarder configuration  
Module 4 - Forwarder management  
Module 5 - Monitor inputs  
Module 6 - Network and scripted inputs  
Module 7 - Fine-tuning inputs  
Module 8 - Parsing phase and data preview  
Module 9 - Manipulating raw data  
Module 10 - Supporting Knowledge objects

Module 11 - Deployment Overview and Licensee management  
Module 12 - Apps  
Module 13 - Configuration File  
Module 14 – Indexes and Index management  
Module 15 - User management  
Module 16 - Configuring Basic Forwarding  
Module 17 - Distributed Search  
Module 18 - Clustering