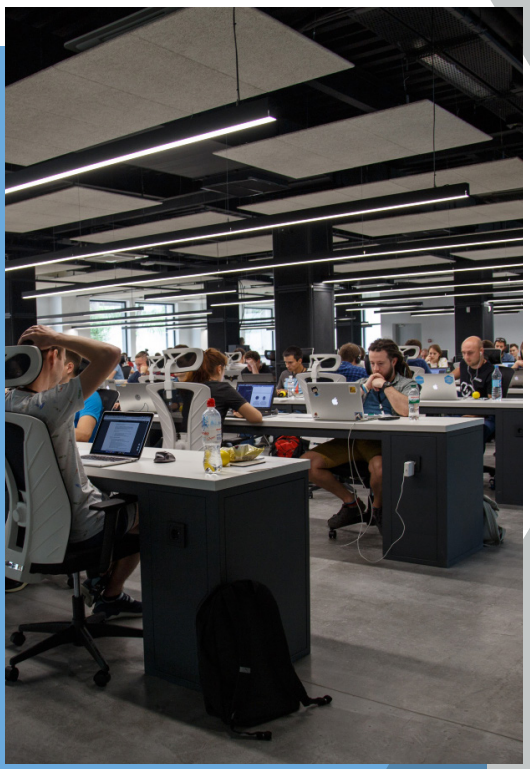
Splunkable
The Splunk Talent Engine

User Fundamentals

Where We Turn _raw Into Talent



Course Outline

Introduction to Splunk

Splunk History, Basics

Splunk Components Introduction and its use

Splunk Installation Windows/Linux

Best practices for production Environment like

- Minimum Recommended hardware requirement
- Factors that affect Splunk processing

User Management and Intro to Conf Files

Managing Users

Understanding Splunk Default Roles (Create/Edit new or existing role)

Mapping role to Splunk User and understanding on Capabilities

Splunk Authentication methods

Configuration Directory Structure

Common Configuration file

(inputs/outputs/indexes/app/web/server/limits/props/transforms etc)

Index Time Precedence Order

Search Time Precedence Order

Data Aging in Splunk

Index architecture (Bucket system Hot/Warm/Cold/Frozen/Thowed)

How data ages in splunk

Data retention policy

Data Archiving policy

Best practices for production Environment

Data Ingestion Into Splunk

Ingest flat file data into Splunk

Understand monitor/upload options

Understanding on Sourcetype

Understand preview page and its settings

Understand settings like line break, timestamp and props.conf file settings

Best practice for prod Environment

Data Ingestion Using Splunk Universal Forwarder

Intro to Splunk Universal forwarder

Installing UF

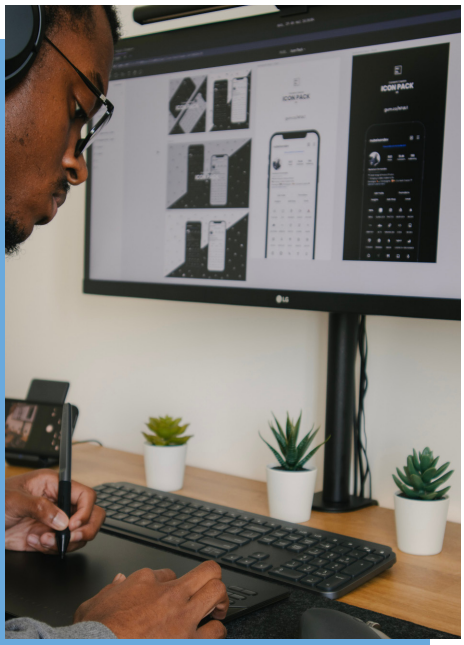
Send data from UF to Indexer

Install DS and manage UF from DS

Push app to UF from DS

Automatic Load balancing

Best practice for prod environment



Knowledge Object I

Understanding on Fields (Interesting/Selected fields)

Field Extraction (via Field extraction utility)

Understanding Regex and Delimiter method

Event Types

Transaction command

Best practice for prod environment

Knowledge Object II

Lookups (file based lookup)

Workflow actions (link, search)

Tags

Field alias

Data model

Best practice for prod environment

Basic Search and Reporting Commands

Understanding on SPL

Commands

fields, table, dedup, rename, sort, search, stats, top, rare, chart, timechart

Best practice for prod environment

Splunk Alerts, Reports and Dashboards

Understanding on (scheduled, real time)

Alert Action understanding

Report creation

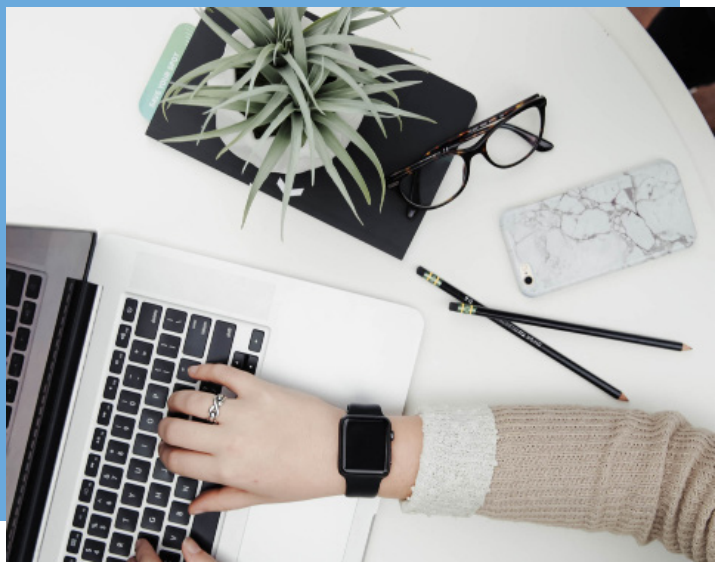
Intro to different visualizations

Creating dashboards

Token concept in Dashboards

Input elements in Dashboards

Drill down feature



Splunkable
The Splunk Talent Engine

Register for Classes Online to Get Started

FOR MORE INFORMATION
SPLUNKABLE.COM
1-844-SPLUNKS