Splunk Development

Module 1 – Start Searching

_____

Introduce Splunk and the Search app

Run basic searches

Identify the contents of search results

Control a search job

Set the time range of a search

Use the output of a search to refine your search

Module 2 – Saving Results and Searches

_____

Export search results

Save and share search results

Saved searches

Schedule searches

Module 3 – Using Fields

_____

Understand fields

Use fields in searches

Use the fields sidebar

Renaming Fields

Fields Alias

Extracting the fields through IFX

Extracting the fields through regular expressions

Module 4 – Tags and Event Types

_____

Understand tags

Create tags and use tags in a search

Describe event types and their uses

Create and use event types in a search

Module 5 – Creating Alerts

_____

Describe alerts

Create an alert

View fired alerts

Automatically exectuing scripts though alerts

Trouble shooting alerts

Module 6 – Creating Reports

_____

Create reports and charts

Create dashboards and add reports

Create and edit dashboards

Add Visualization to the dashboards

Permission of the dashboard

Conversion of basic XML to advance XML and its usage

Conversion of basic XML to HTML and its usage

Using Inline searches and saved searches in dashboards

Module 7 - Reporting Commands

_____

Using different reporting commands and their functions eg -Top, Rare, Stats, etc

Explore the available visualizations

Create a basic chart

Split values into multiple series

Omit null and other values from charts

Create a timechart

Chart multiple values on the same timeline

Format charts

Explain when to use each type of reporting command

Module 8 - Analyzing, Calculating, and Formatting Results

_____

Using the eval command

Perform calculations

Convert values

Round values

Format values

Use conditional statements

Further filter calculated results

Module 9 - Enriching Data with Lookups

_____

Describe lookups

Examine a lookup file example

Create a lookup table

Define a lookup

Use the lookup in searches and reports

Splunk Admin

Module 1 : Installing Splunk

_____

Splunking: What does it Mean ?

How Should Splunk be Configured ?

Identifying Splunk Instance Types

Hardware Recommendations - Indexers

Hardware Recommendations - Search Heads

Splunk Install Packages

Supported Platforms and Browsers

Installation

Splunk Directory Structure

The Splunk Command Line Interface

*NIX - Run Splunk at Boot

Splunk Windows Services

Splunk Processes : Splunkd

Splunk Processes : Splunk Web

Apps Installed by Default

System Settings

Describing General Settings

Restarting the Server from Splunk Web

Module 2 : License Management

_____

Managing Licenses

Splunk License Types

Adding a License

License Warnings and violations

What Counts As Daily License Quota

Viewing Alerts

License Staking

Master License Server

License Pooling

Module 3 : Basic Data Input

_____

Adding an Input With Splunk Web

How can you tell what App you are in ?

Adding your Monitor Input

Preview Data

Specify the Source

Select Host, Sourcetype and Index

Module 4 : Managing Apps

_____

What is an App ?

Apps configured by Default

Viewing All Apps

Managing Apps

Installing an App from Splunk site

Installing an App Manually

Enabling and Disabling Apps

Deleting an App

App Permissions

Module 5 : Splunk Configuration Files

_____

Configuration Directories

Default vs. Local Configuration

Global Context vs. User or App Context

Runtime Merging of Configurations

Configuration Testing Commands

Using btool

Reloading Configuration Files After Edit

Module 6 : Universal Forwarders

_____

Forwarders and Indexers

Benefits of Using Forwarders

Splunk Universal Forwarder

Heavy Forwarder

Configuration Steps

Configuring the Receiving Port

Downloading the Universal Forwarder Installer

Installing Universal Forwarder Manually

Forwarder Configuration Files

Defining Target Indexer on the Forwarder

Testing the Connection

Automatic Load Balancing

Caching/Queue Size in outputs.conf

Indexer Acknowledgement

Configuring Forwarder Inputs

Module 7 : Overview of Inputs

_____

Typical Data Input Scenarios

Data Input Types

Splunk Index Time Process

Default Metadata Settings

Understanding Sourcetypes

Manual vs. Automatic Sourcetyping

Module 8 : Monitor Inputs

_____

Monitoring Files and Directories

Monitor Input Syntax

File Pathname Wildcards

File and Directory Matching

Using Whitelist to Include Files

Using Blacklist to Exclude Files

Module 9 : Splunk Indexes

_____

What are Indexes ?

Default Index: Main

Other Preconfigured Indexes

Why Create Your Own Indexes ?

Managing Indexes with Splunk Web

What is indexes.conf ?

Module 10 : Index Maintenance and Optimization

_____

Viewing Indexing Activity

Inspecting Buckets (dbinspect)

What to Backup

Backup Recommendation

Moving an Entire Index: Checklist

indexes.conf Only Options

Removing Indexed Data

Deleting Events

Cleaning out an Index

The Fishbucket

Restoring a Frozen Bucket