Splunk Table of Content (8 Full Days)			
Day	**Module**	**Topics**	**Mode**
Day - 1	**Module - 1**	What is Splunk	Theory
		How Splunk Started	Theory
		Splunk Overview	Theory
		Splunk Real Time Examples	Theory
		Splunk Deployment Methods	Theory + Lab
		Splunk Installation Lab	Theory + Lab
	Module - 2	Data Input in Splunk	Theory + Lab
		Splunk UI Overview	Theory + Lab
		Creating and scheduling searches	Theory + Lab
		Demo - Searches	Theory + Lab
		Creating and scheduling Alerts	Theory + Lab
		Demo - Alerts	Theory + Lab
		Splunk Alert Integration with Multiple tools	Theory + Lab
		Lab on Module 2	Theory + Lab
	Module - 3	Splunk searches and reporting commands	Theory + Lab
		stats	Theory + Lab
		field	Theory + Lab
		table	Theory + Lab
		rex	Theory + Lab
		rename	Theory + Lab
		where	Theory + Lab
		top	Theory + Lab
		rare	Theory + Lab
		addcoltotals	Theory + Lab
		chart	Theory + Lab
		timechart	Theory + Lab
		Eventcount	Theory + Lab
Day - 2	**Module - 4**	Splunk Knowledge objects	Theory + Lab
		saved searches	Theory + Lab
		event types	Theory + Lab
		tags	Theory + Lab
		field extractions	Theory + Lab
		lookups	Theory + Lab
		reports	Theory + Lab
		alerts	Theory + Lab
		Alert Integrating with ITSM (ServiceNow)	Theory + Lab
		Transactions	Theory + Lab
		data model	Theory + Lab
		fields	Theory + Lab
		workflow actions	Theory + Lab

Day - 3	**Module - 5**	Enriching Data with Lookups	Theory + Lab
		Correlating Events	Theory + Lab
		Analysing, Calculating and Formatting Results	Theory + Lab
		Data Model Implementation	Theory + Lab
		Performance Improvement Splunk Queries	Theory + Lab
		Best practice for Splunk Queries	Theory + Lab
	Module - 6	Splunk System Administration	Theory + Lab
		Splunk Deployment Overview	Theory + Lab
		Splunk Engine Architecture	Theory + Lab
		Splunk Deployment Architecture	Theory + Lab
		Upgrading Splunk	Theory + Lab
		Disaster Recovery	Theory + Lab
		Scaling Splunk architecture (upscaling and downscaling)	Theory + Lab
Day - 4	**Module - 7**	Splunk License Management	Theory + Lab
		Splunk License Types	Theory + Lab
		License Warnings and Violations	Theory + Lab
		Add / Remove Licenses	Theory + Lab
		Splunk License Master-Slave setup	Theory + Lab
		Splunk License Pools	Theory + Lab
	Module - 8	Splunk Apps & Add-Ons	Theory + Lab
		Concept and Pre-Requisites	Theory + Lab
		Installation and Configuration	Theory + Lab
		Fine-tuning and Uninstallation	Theory + Lab
		Creating a Sample Splunk App	Theory + Lab
		Developing custom add-ons	Theory + Lab
	Module - 9	Splunk Configuration Files	Theory + Lab
		Most frequently used/accessed files	Theory + Lab
		Config file extensions, structure	Theory + Lab
		Config File Precedence	Theory + Lab
Day - 5	**Module - 10**	Splunk Indexes	Theory + Lab
		Concept of Splunk Indexes	Theory + Lab
		Splunk Index structure	Theory + Lab
		Create and configure new Indexes (UI, CLI & Conf file methods)	Theory + Lab
		Monitor Splunk Indexes using MC	Theory + Lab
	Module - 11	Splunk User Management	Theory + Lab
		Splunk Users and Roles	Theory + Lab
		Creating custom Users and Roles	Theory + Lab
		Verify / Test custom capabilities	Theory + Lab
	Module - 12	Splunk Authentication Methods	Theory + Lab
		Understand various options of Authentication	Theory + Lab

		Walk-through screens for LDAP, SAML and MFA	Theory
	Module - 13	Receiving Data in Splunk	Theory + Lab
		Overview of Data Inputs	Theory + Lab
		Basic Settings for input options	Theory + Lab
		Examples and use-cases of different methods	Theory + Lab
	Module - 14	Scaling your Splunk Deployment	Theory
		Overview Distributed Search	Theory
		Overview of Splunk Indexer Cluster	Theory
		Overview of Splunk Search Head Cluster	Theory
		Overview of Deployment Server	Theory
Day - 6	**Module - 15**	Splunk Forwarders	Theory + Lab
		Overview & Types of Splunk Forwarders	Theory + Lab
		Install Splunk UF	Theory + Lab
		Introduction to Splunk Forwarder Mgmt UI	Theory + Lab
		Introduction to Splunk Deployment Server	Theory + Lab
		Configure Server Classes and Deployment Apps	Theory + Lab
Day - 7	**Module - 16**	Monitor Inputs	Theory + Lab
		Create F&D monitor inputs	Theory + Lab
		Deploy remote monitor inputs using UF	Theory + Lab
		Overview of Network, Windows and Other types of inputs	Theory + Lab
		Onboarding logs via Syslog servers for SNMP traps, toll, and SFTP logs	Theory + Lab
		Onboarding logs using custom Python scripts	Theory + Lab
		Onboarding logs using CSV Splitters	Theory + Lab
		Data Onboarding using ServiceNow Add-on	Theory + Lab
Day - 8	**Module - 17**	Basic understanding of Splunk ITSI	Theory
		Basic understanding of Splunk ES	Theory
	Module - 18	Closure Note	
		Tip & Tricks	
		Notes	