Splunk Analyst
Basics to Advanced Course

Duration
40 hours (05 full days)

Prerequisites
1. Basic Linux Commands
2. Basic understanding of XML Tags
3. Basic Understanding of Json format

Course Overview
This comprehensive 5-day Splunk Analyst course covers the basics to advanced concepts of Splunk. Participants will learn about Splunk's history, architecture, and deployment, followed by practical labs on data input, search creation, and alert scheduling. The course delves deeper into Splunk's powerful searching, reporting commands, and knowledge objects. Advanced topics include system administration, license management, custom add-ons, and dashboard optimizations. This training equips learners with the skills to efficiently use and manage Splunk in real-world scenarios.

Course Outline

Splunk Table of Content (5 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 (Using Database and String detection)	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
			reports	Theory + Lab
			alerts	Theory + Lab
			Transactions	Theory + Lab
			data model	Theory + Lab
			fields	Theory + Lab
			workflow actions	Theory + Lab
		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
Day - 3		**Module - 6**	Splunk System Administration	Theory + Lab
			Splunk Deployment Overview	Theory + Lab
			Splunk Engine Architecture	Theory + Lab
			Splunk Deployment Architecture	Theory + Lab
		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
		Developing custom add-ons	Theory + Lab
Day - 4	**Module - 9**	Classic Dashboard	Theory + Lab
		Static and Dynamic Dashboard creation	Theory + Lab
		Input Creation	Theory + Lab
		Event Handler	Theory + Lab
		Optimization of Dashboard	Theory + Lab
Day - 5	**Module - 10**	Studio Dashboard	Theory + Lab
		Input Creation	Theory + Lab
		Flowchart Creation	Theory + Lab
		Optimization of Dashboard	Theory + Lab
	Module - 11	Closure Note	
		Tip & Tricks	
		Notes	