Splunk Dev & Admin (Cyber Security)

Thank you for contacting our **SQL School**. I am **Mr. Sai Phanindra**, trainer for this **Splunk** Course. With 20 Years of technical expertise exclusively on Database, Big data & Network, I assure you 100% Practical, Step by Step Classes for this **Splunk** course.
My Profile @ https://www.linkedin.com/in/saiphanindra/

What is Cyber Security?

Cybersecurity is the practice of protecting computer systems, networks, and data from digital attacks, damage, or unauthorized access, defend against threats like malware, phishing, ransomware and ensure 24 x 7 availability of information securely.

What is Splunk?

Splunk is a big data platform that simplifies the task of collecting and managing massive volumes of machine-generated data and searching for information within it. The technology is used for business and web analytics, application management, compliance, and security.

What are the Job Roles in Splunk?

- **Splunk Engineer**
- **Splunk Administrator**
- **Splunk Analyst**
- **Cyber Security Analyst**
- **SIEM Engineer**
- **Site Reliability Engineer**

Who can join this course?
Anyone. There are NO Pre-requisites for this course. I will teach you from the very basics of Data, Network, Security and Analytics in this course, step by step !!

Cyber Security : Splunk SOC Training:
- **Module 1: Splunk Concepts, Dev**
- **Module 2: Splunk Admin**

Trainer: linkedin.com/in/saiphanindra/

Total Duration: 1.5 Months
Realtime Project: Included
Resume Guidance: Included

This course is very helpful for:
1. Cyber Security Professionals
2. Security Admins
3. Network Admins
4. Consultants
5. Architects

Detailed Course Content

Module 1: Splunk Concepts

Ch 1: Cyber Security Introduction
- ✓ What is Cyber Security?
- ✓ Cyber Security Concepts
- ✓ On-Premise & Cloud Security

Ch 2: Introduction to Splunk
- ✓ What is Splunk?
- ✓ Basic overview of Splunk
- ✓ Splunk architecture

Ch 3: Splunk Installations
- ✓ Splunk Implementations
- ✓ Splunk in On-Premises
- ✓ Installing, Configuring Splunk
- ✓ Spunk UI - Usage

Ch 4: Splunk Operations - Level 1
- ✓ Splunk Search Concepts
- ✓ Basic Search
- ✓ Refine search

- ✓ Time range

Ch 5: Splunk Operations - Level 2

- ✓ Auto Complete Search
- ✓ Search Job Controls
- ✓ Search Content Consolidation
- ✓ Search Content Reporting

Ch 6: Fields in Searches

- ✓ Fields in Searches Concept
- ✓ Search Architecture
- ✓ Deploying Fields sidebar
- ✓ Using Field Extractor
- ✓ FX to delimited Field extraction

Ch 7: Search Schedules

- ✓ Writing queries for Search
- ✓ Sharing search results
- ✓ Saving Search Results
- ✓ Scheduling and exporting search issues

Ch 8: Reporting Commands

- ✓ Add coltotals functions
- ✓ Add totals functions
- ✓ Top Functions
- ✓ rare and stats Functions

Ch 9: Splunk Visualization

- ✓ Overview of Visualization
- ✓ Creation of charts
- ✓ Time Charts
- ✓ Format results
- ✓ Omit null values

Ch 10: Building Reports and Dashboards

- ✓ Building search charts, and dashboards
- ✓ Making changes to reports and dashboards
- ✓ Adding reports to dashboards

Ch 11: Tags and Events

- ✓ Overview of Tags in Splunk
- ✓ Using Tags in Splunk search
- ✓ Overview of various event types
- ✓ Introduction to event types and utility
- ✓ Creation, implementation of event types

Ch 12: Developing and using Macros

- ✓ Introduction to Macro
- ✓ Variables in Macro
- ✓ arguments in Macros

Ch 13: Workflow

- ✓ Workflow creation
- ✓ search workflow actions
- ✓ Post workflow actions

Ch 14: Splunk Search Commands

- ✓ Introduction to the search command
- ✓ Understanding search
- ✓ What is a search pipeline
- ✓ Highlighting the syntax
- ✓ The process to specify the index in search
- ✓ Deploying commands like tables, sort, fields, rename, sort, and rex.

Ch 15: Analysing, Calculating and Formatting Results

- ✓ Calculation of results
- ✓ Analysis of results
- ✓ Value conversion
- ✓ Format values
- ✓ Roundoff
- ✓ Conditional statements
- ✓ Using the eval command
- ✓ Filtering search results

Ch 16: Data Lookups

- ✓ Understanding Data Lookups
- ✓ Lookup Tables
- ✓ Configuring automatic Lookups
- ✓ Deploying Lookups in Searches
- ✓ Deploying reports in reports

Ch 17: Common Information Model

- ✓ Overview of Splunk SIM model
- ✓ Using CIM to normalize data1

Ch 18: Single Value and Mapping Commands

- ✓ Geostats, geom
- ✓ Iplocation
- ✓ Addtotals commands

Module 2: Splunk Admin

Ch 19: Distributed Management Console

- ✓ Basics of Splunk Distributed Management Console
- ✓ Cluster indexing
- ✓ Process to deploy distributed search in Splunk
- ✓ User authentication and monitoring
- ✓ Forward Management

Ch 20: Splunk App

- ✓ The need for Splunk Apps
- ✓ Procedure to develop Splunk applications
- ✓ Splunk App add-ons
- ✓ Splunk base Concepts
- ✓ The process to use Splunk apps
- ✓ App permissions and deploying
- ✓ Apps on-forwarder

Ch 21: Splunk Indexes and users

- ✓ Data of index time configuration file
- ✓ Overview of search time configuration file

Ch 22: Splunk Configuration Files

- ✓ Forward Installation
- ✓ Search time and index time configuration
- ✓ Universal Forwarder management
- ✓ Input and output configuration

Ch 23: Splunk Deployment Management

- ✓ Implementation of Splunk tool
- ✓ Splunk Deployment on the server
- ✓ Setting up the Splunk environment
- ✓ Splunk client group deployment

Ch 24: Splunk Indexes

- ✓ Overview of Splunk Indexer
- ✓ Separating the Splunk indexes
- ✓ Overview of Splunk
- ✓ Index storage estimation

Ch 25: User role and Authentication

- ✓ A brief overview of role inheritance
- ✓ Splunk Authentications
- ✓ LDAP authentications
- ✓ Native authentications

Ch 26: Splunk Administration Environment

- ✓ Data Inputs
- ✓ Splunk important concepts
- ✓ App management
- ✓ Search indexer and forwarder
- ✓ Parsing machine-generated data

Ch 27: Production environment

- ✓ Overview of Splunk configuration files

- ✓ Data management
- ✓ Solving issues and continuous monitoring

Ch 28: Splunk Search Engine

- ✓ Machine-generated data : operational intelligence
- ✓ Configuring reports, dashboards, and charts
- ✓ Indexer Clustering and Search Head Clustering

Ch 29: Different Splunk Input Methods

- ✓ Overview of various input methods
- ✓ Deploying a scripted network and windows
- ✓ Overview of Agentless inputs

Ch 30: Splunk User and Index Management

- ✓ User authentication
- ✓ Role assigning
- ✓ Administering Splunk indexes

Ch 31: Splunk Cluster Implementation

- ✓ Introduction to Cluster indexing
- ✓ Cluster behaviour configuration
- ✓ Individual nodes configuration
- ✓ Configuring Search Behaviour
- ✓ Handling a peer node, a master node, and a search head.

Ch 32: Splunk Cluster Implementation

- ✓ Introduction to Cluster indexing
- ✓ Cluster behaviour configuration
- ✓ Individual nodes configuration
- ✓ Configuring Search Behaviour
- ✓ Handling a peer node, a master node, and a search head.

Ch 33: Project Work for your Resume (Banking Domain)

- ✓ **Enrol for a LIVE Demo. Interact with our trainer before you proceed.**
  - 👉 **Reach Us: +91 9666 64 0801**
    +91 9666 44 0801
  - 👉 **Website: www.sqlschool.com**
  - 👉 **Youtube**: www.youtube.com/sequelschool
  - 👉 **Training Modes: LIVE Online / Self Paced Videos**

- ✓ **Thank you for your time, wish you all the very best !!**