Splunk Course Table of content.

1. Introduction to Splunk
    - What is Splunk?
    - Splunk architecture and components
    - Use cases and benefits of Splunk
    - Getting started with Splunk
2. Installing and Configuring Splunk
    - System requirements and hardware considerations
    - Installation options and deployment scenarios
    - Splunk licensing and editions
    - Configuration files and settings
    - Splunk web interface overview
3. Searching and Reporting in Splunk
    - Basic search commands and syntax
    - Search filters and operators
    - Time range and field extractions
    - Using fields and aliases in searches
    - Creating and modifying search queries
    - Introduction to Splunk Search Processing Language (SPL)
4. Indexing and Data Input
    - Indexing fundamentals and concepts
    - Data input options (files, directories, network, etc.)
    - Configuring data inputs and source types
    - Data parsing and event processing
    - Data preview and troubleshooting
5. Splunk Search Language (SPL)
    - Advanced search commands and functions
    - Transforming search results
    - Statistics and aggregation commands
    - Time series analysis and forecasting
    - Correlation and anomaly detection
6. Creating Dashboards and Visualizations
    - Introduction to Splunk dashboards
    - Building panels and visualizations
    - Charting and graphing options
    - Layouts and formatting options
    - Dashboard drilldown and interactivity
7. Alerts and Notifications
    - Setting up alerts and triggers
    - Alert actions and configurations

- Custom alert scripts
- Event forwarding and data distribution
- Configuring notifications and actions

8. Splunk Administration and Security
    - User management and authentication
    - Roles and permissions in Splunk
    - Splunk data management and retention
    - Monitoring and troubleshooting Splunk
    - Security best practices and considerations
9. Splunk App Development
    - Overview of Splunk app framework
    - App development environment and tools
    - Creating custom dashboards and visualizations
    - Packaging and distributing Splunk apps
    - App deployment and versioning
10. Splunk Enterprise Security
    - Introduction to Splunk Enterprise Security
    - Security information and event management (SIEM)
    - Threat intelligence and incident response
    - Monitoring and detecting security threats
    - Creating security reports and investigations