Splunk the centralized log management system:

Duration: 24 hours
Hello world this is me

Day 1: Splunk Administration Fundamentals (8 Hours)

Module 1: Introduction to Splunk (1 Hour)
- Overview of Splunk
- Key Features and Benefits
- Use Cases and Applications
- Splunk Architecture: Overview of Search Head, Indexers, and Forwarders

Module 2: Splunk Installation and Configuration (3 Hours)
- Installation Requirements and Prerequisites
- Splunk Installation on Hardware
- Splunk Installation in Containers
- Splunk Licensing
- Understanding Splunk Licensing
- Managing Licenses
- Initial Setup and Configuration
- Configuration Files Overview
- Managing Splunk Indexes
- User Management and Roles
- Setting Up Data Inputs and Forwarders

Module 3: Splunk User Interface Introduction (1 Hour)
- Navigating the Splunk UI
- Key UI Components
- Customizing the Splunk Dashboard

Module 4: Splunk Indexes and Search Engine (1 Hour)
- Understanding Splunk Indexes
- Managing Indexes
- Search Engine Fundamentals

Module 5: Splunk Configuration Management (2 Hours)

- Introduction to Splunk Configuration Files
- Universal Forwarder and Forwarder Management
- Distributed Management Console
- Data Management and Troubleshooting
- Labs and Use Cases:
- Lab 1: Installing Splunk on a Virtual Machine

- Lab 2: Configuring Splunk in a Docker Container
- Lab 3: Setting Up and Managing Splunk Forwarders

Day 2: Advanced Splunk Searching and Reporting (8 Hours)

Module 6: Searching in Splunk (1 Hour)
- Basic Search Commands
- Search Fundamentals
- Using Fields in Searches

Module 7: Advanced Search Commands (2 Hours)
- Reporting Commands
    - Top
    - Rare
    - Stats
    - Addcoltotals
- Advanced Commands
    - Join
    - Lookup
    - Transaction
    - Xyseries
    - Streamstats
    - Eventstats
    - Bin

Module 8: Creating Reports and Visualizations (2 Hours)
- Explore Available Visualizations
- Create Basic Charts
- Split Values into Multiple Series
- Omit Null and Other Values from Charts
- Create a Timechart
- Chart Multiple Values on the Same Timeline
- Format Charts

Module 9: Working with Dashboards (1 Hour)
- Creating and Managing Dashboards
- Dynamic Dashboard Creation

Module 10: Creating and Managing Alerts (1 Hour)
- Setting Up Alerts
- Managing Alert Conditions and Actions

Module 11: Using Macros and Field Aliases (1 Hour)
- Creating and Using Macros

- Creating Field Aliases
- Labs and Use Cases:
- Lab 4: Creating and Managing Indexes and User Roles
- Lab 5: Ingesting and Searching Data with Splunk
- Lab 6: Creating Reports and Visualizations

Day 3: Advanced Splunk Features and Management (8 Hours)

Module 12: Data Model and Pivot (1 Hour)
- Understanding Data Models
- Creating and Managing Data Models
- Using Pivot for Data Analysis

Module 13: Splunk REST API (1 Hour)
- Introduction to Splunk REST API
- Common API Endpoints and Usage
- Building Applications with Splunk API

Module 14: Scaling and Monitoring Splunk (2 Hours)
- Best Practices for Scaling Splunk
- Monitoring Splunk Performance
- Troubleshooting Common Issues

Module 15: Splunk's Distributed Environment (1 Hour)
- Overview of Distributed Splunk Deployment
- Managing Search Head Clusters
- Managing Indexer Clusters

Module 16: Advanced Data Management (2 Hours)
- Advanced Forwarder Management
- Data Retention Policies
- Data Backup and Recovery

Module 17: Introduction to Splunk Configuration Files (1 Hour)
- Deep Dive into Configuration Files
- Common Configuration Tasks
- Best Practices for Configuration Management
- Labs and Use Cases:
- Lab 7: Advanced Search Techniques
- Lab 8: Configuring Alerts and Dashboards
- Lab 9: Using Splunk REST API for Automation
- Lab 10: Scaling and Monitoring Splunk