Splunk Content

- Splunk Introduction

- Splunk Deployment
  - Deployment Models
  - Licensing Models
  - Understanding Licensing

- Installing Splunk
  - Provisioning a Splunk on AWS Cloud Instance
  - Provisioning a Splunk on AWS Cloud practical
  - Linux basic admin part for Splunk installation
  - Download and install Splunk on Linux theory
  - Download and install Splunk on Linux practical
  - Download and install Splunk on Windows theory
  - Download and install Splunk on Windows practical

- Getting data In
  - How many ways data can retrieve into the Splunk
  - What is Universal Forwarders
  - Universal Forwarder practical
  - What is Heavy Forwarder
  - Heavy Forwarder practical
  - Installing Forwarders in different OS and getting data in

- Search and Reporting
  - The Search App
  - The search pipeline
  - Basic searching
  - Dealing with time
  - Search modes
  - Search Fields
  - Filed Discovery
  - Filtering and formatting
  - Fields aliases
  - Fields extractors
  - Fields Count

- Visualizing your data
  - Data Models
  - What is Pivot
  - Using Pivot to Build Basic Visualizations
  - Chart and Time Chart commands

    - Reporting and Alerting

- Advanced Splunk Concepts
    - Users, Roles and Authentication
    - Configuration Files
    - Knowledge Objects
    - Lookups
    - Advanced search commands and Functions