Splunk Intermediate Training

Curriculum 3 Days

Day - 1

- **What Is Splunk?**
  - What Is Splunk?
  - Overview
  - Machine Data
  - Splunk Architecture
  - Careers in Splunk
  - Summary
- **Setting up the Splunk Environment**
  - Overview
  - Splunk Licensing
  - Getting Splunk
  - Installing Splunk
  - Adding Data to Splunk
  - Summary
- **Basic Searching Techniques**
  - Overview
  - Demo: Adding More Data
  - Search in Splunk
  - Demo: Splunk Search
  - Splunk Search Commands
  - Demo: Splunk Processing Language
  - Splunk Reports
  - Demo: Reporting in Splunk
  - Splunk Alerts
  - Demo: Alerts in Splunk
  - Summary
- **Enterprise Splunk Architecture**
  - Overview
  - Forwarders
  - Enterprise Splunk Architecture
  - Installing Forwarders
  - Demo: Installing Forwarders
  - Demo: Troubleshooting Forwarder Installation
  - Summary

Day - 2

- **Splunking for DevOps and Security**
  - Overview
  - Splunk in DevOps
  - DevOps Demo
  - Splunk in Security
  - Enterprise Use Cases
  - Summary
- **Application Development in Splunkbase**
  - Overview
  - What Is Splunkbase?
  - Navigating the Splunkbase
  - Creating Apps for Splunk
  - Benefits of Building in Splunkbase
  - Summary

- **Splunking for DevOps and Security**
  - Overview
  - Splunk in DevOps
  - DevOps Demo
  - Splunk in Security
  - Enterprise Use Cases
  - Summary
- **Application Development in Splunkbase**
  - Overview
  - What Is Splunkbase?
  - Navigating the Splunkbase
  - Creating Apps for Splunk
  - Benefits of Building in Splunkbase
  - Summary

Day - 3

- **Composing Advanced Searches**
  - Introduction to Advanced Searching
  - Eval and Fill null Commands
  - Other Splunk Command Usage
  - Filter Those Results!
  - The Search Job Inspector
  - Summary
- **Generating Visualizations Using Commands**
  - Introducing Splunk Visualizations
  - Visualization Data Structures
  - What Do You Want to See?
  - Transforming Commands
  - Single Value, Maps, and Gauges
  - Summary
- **Creating Search Macros**
  - What Are Search Macros?
  - Using Search Macros within Splunk
  - Macro Command Options and Arguments
  - Other Advanced Searching within Splunk
  - Summary
- **Course Summary**
  - Course Review
  - Case Study: Advanced Searching with Splunk
  - Let's Wrap!