Course duration

- 2 days

Course Benefits

- Splunk components
- Data sources
- SPL
- Forwarders
- Data visualizations

Course Outline

1. Splunk Introduction
    1. Splunk Defined
    2. Splunk Products
    3. The Magic Quadrant for Security Information and Event Management (SIEM)
    4. Splunk Editions
    5. Deployment Options
    6. Common Components
    7. Splunk Admin Dashboard (Web UI)
    8. Events
    9. Data Indexing
    10. Distributed Splunk Indexing and Searching
    11. Architecture for a Multi-Tier Splunk Enterprise Deployment
    12. Summary
2. Splunk Data Sources
    1. Data Source Types
    2. The Source Types Automatically Recognized by Splunk
    3. The “Pre-trained” Source Types
    4. Windows ® Data Sources
    5. Data Indexing
    6. Web UI for Adding Data to Indexer
    7. Web UI: Adding Data Flow for Local File Upload
    8. Web UI: Add Data for Monitoring
    9. Automatic Recognition of Data Source
    10. Where is My Uploaded File?
    11. Custom Event Format
    12. Summary
3. Searching and Reporting with Splunk
    1. Data Searching

2. The Search Processing Language (SPL)
3. Searching and Reporting Activities
4. The Search Page
5. Core Search Concepts
6. Search Command Auto-Completion
7. The Search Basics
8. Search Command Categories
9. Command Examples
10. More Examples of Search Commands
11. Statistical Commands
12. Statistical and Time Functions
13. From SQL to SPL – the Translation Table
14. Visual Aids for Building Search Queries
15. Visualizations
16. Save Your Searches as Dashboards
17. The Delete Operation
18. How Do I Delete My Data?
19. Summary

4. Splunk Forwarders
    1. Flavors of Splunk Forwarders
    2. Forwarder Comparison Table (Abridged)
    3. The Splunk Forwarder Diagram
    4. Splunk Universal Forwarder (UF) Supported OSes
    5. UF Functions
    6. What UF Cannot Do
    7. Summary

Class Materials

Each student will receive a comprehensive set of materials, including course notes and all the class examples.

Class Prerequisites

Experience in the following *is required* for this Hadoop class:

- General knowledge of programming using SQL as well as some experience working in UNIX environments (e.g., running shell commands, etc.).