Security Through Mining Log Using Splunk

Curriculum 2 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 Langauge
  - 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

- **Security Through Mining Log Using Splunk**
  - 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 on Hadoop with Hunk**
  - Overview
  - What Is Hadoop?
  - Demo: Running HDFS Commands
  - What Is Hunk?
  - Demo: Installing Hunk
  - Demo: Moving Data from HDFS to Hunk
  - Summary