

Splunk Training

Level - Advance



April 26, 2020

Cotocus Ltd.

Bangalore, India

|  |  |
| --- | --- |
| Training Dates | TBD |
| Time | TBD |
| Trainer Name | Rajesh Kumar |
| Number of Days | 5 Day |

Agenda

Day 1

**What Is Splunk?**

* What Is Splunk?
* Overview
* Machine Data
* Splunk Architecture
* Careers in Splunk

**Setting up the Splunk Environment**

* Overview
* Splunk Licensing
* Getting Splunk
* Installing Splunk
* Adding Data to Splunk

**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

**Enterprise Splunk Architecture**

* Overview
* Forwarders
* Enterprise Splunk Architecture
* Installing Forwarders
* Demo: Installing Forwarders
* Demo: Troubleshooting Forwarder Installation

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 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

Day 3

**Composing Advanced Searches**

* Introduction to Advanced Searching
* Eval and Fillnull Commands
* Other Splunk Command Usage
* Filter Those Results!
* The Search Job Inspector

**Generating Visualizations Using Commands**

* Introducing Splunk Visualizations
* Visualization Data Structures
* What Do You Want to See?
* Transforming Commands
* Single Value, Maps, and Gauges

**Creating Search Macros**

* What Are Search Macros?
* Using Search Macros within Splunk
* Macro Command Options and Arguments
* Other Advanced Searching within Splunk
* Case Study: Advanced Searching with Splunk

Day 4

**Introduction**

* Course Introduction
* Course Overview
* What is Machine Data?
* What Are We Working With?

**Optimizing Splunk Knowledge**

* Introduction to Knowledge
* Knowledge Objects and Categorization
* Data Enrichment and Data Models
* Naming Conventions
* Managing Knowledge Objects

**Managing Splunk Fields**

* What Are Fields?
* All Things Fields
* The Field Extractor
* Creating and Using Fields
* Creating and Using Calculated Fields

**Using Tags and Event Types**

* Tags and Event Types
* Tags and Events
* Creating and Using Tags
* Creating and Using Event Types

Day 5

**Getting Familiar with Data Models and the Pivot Tool in Splunk**

* Who Is a Splunk Knowledge Manager?
* Introducing the Splunk Pivot Tool
* What Is a Data Model?
* Demo: Introduction to Pivot

**Diving Deeper into Data Models**

* The Benefits of Modeling Data
* The Ingredients of a Data Model
* Data Model Acceleration
* Data Model Configuration Files
* Demo: Explore an Existing Data Model

**Identifying Data Model Attributes**

* Overview
* Data Model Datasets
* Dataset Field Categories
* Field Extractions
* Our Scenario
* Creating a Data Model that will Satisfy our Business Requirements, Part 1
* Creating a Data Model that will Satisfy our Business Requirements, Part 2
* Creating a Data Model that will Satisfy our Business Requirements, Part 3

**Building Dashboards, Reports, and Alerts Using the Data Model**

* Pivot Table Elements
* Visualization Types and Their Uses
* Creating a Dashboard, Reports, and Alerts from our Data Model, Part 1
* Creating a Dashboard, Reports, and Alerts from our Data Model, Part 2
* Creating a Dashboard, Reports, and Alerts from our Data Model, Part 3
* Creating a Dashboard, Reports, and Alerts from our Data Model, Part 4
* Creating a Dashboard, Reports, and Alerts from our Data Model, Part 5
* Creating a Dashboard, Reports, and Alerts from our Data Model, Part 6