splunk>

Creating Splunk 6 Knowledge Objects

Are you in charge of creating Splunk knowledge objects for your organization? Then you will benefit from this 9-hour course that walks you through the various knowledge objects and how to create them. Using a dedicated lab environment, reinforce what you've learned with hands on exercises.

Course Topics

- Lookups
- Fields (Field aliases, field extractions, calculated fields)
- Tags and Event Types
- Workflow Actions
- Alerts
- Scheduled Reports
- Macros
- Data Models

Course Prerequisites

Using Splunk, Searching and Reporting with Splunk.

Class Format

Instructor-led lecture with labs. Delivered via virtual classroom or at your site.

Course Objectives

Module 1 – Introduction

- Overview of Buttercup Games Inc.
- Lab Environment

Module 2 – Implementing Knowledge Objects

- Describe the Common Information Model (CIM)
- Understand the relationship between the CIM and knowledge objects
- Define naming conventions
- Review permissions

Module 3 – Creating Lookups

- Describe lookups
- Create a lookup file and create a lookup definition
- Configure an automatic lookup

Module 4 – Creating Field Aliases and Calculated Fields

- Create and use field aliases
- Create and use calculated fields

Module 5 – Creating Field Extractions

- Perform regex field extractions using the Field Extractor (FX)
- Perform delimiter field extractions using the FX

Module 6 – Creating Tags and Event Types

- Create and use tags
- Describe event types and their uses
- Create an event type

Module 7 – Creating Workflow Actions

- Describe the function of GET, POST, and Search workflow actions
- Create a GET workflow action
- Create a Search workflow action

Module 8 – Creating Alerts and Scheduled Reports

- Describe alerts
- Create alerts
- View fired alerts
- Describe scheduled reports
- Configure scheduled reports

Module 9 – Creating and Using Macros

- Describe macros
- Create and use a basic macro
- Define arguments and variables for a macro
- Add and use arguments with a macro

Module 10 – Creating Data Models

- Describe the relationship between data models and pivot
- Identify data model attributes
- Create a data model
- Use a data model in pivot

About Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all of Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/goto/education

To contact us, email education_AMER@splunk.com

About Splunk

Splunk is software that indexes, manages and enables you to search data from any application, server or network device in real time.

Visit our website at www.splunk.com to download your own free copy.

Splunk Inc.
250 Brannan
San Francisco, CA 94107
866.GET.SPLUNK
(866.438.7758)
sales@splunk.com
support@splunk.com