Splunk Data Onboarding

Course Summary

Description

The “Splunk Data Onboarding” course is targeted for beginner and intermediate users of Splunk. After completing this course, students will have an understanding for bringing data into Splunk using best practices. The course will also cover how to add knowledge objects once the data has been boarded, creating alerts, scheduling reports, using data models and the Common Information Model. This course contains 10 labs for users to practice concepts they have learned during the course.

Topics

- Lookups
- Fields
- Props and Transforms
- Tags and Event Types
- Workflow Actions
- Alerts
- Scheduled Reports
- Macros
- Data Models
- Common Information Model

Audience

The “Splunk Data Onboarding” course is targeted for beginner and intermediate users of Splunk.

Prerequisites

Before taking this course, students should have taken the Splunk User course.

Duration

One day

ProTech protechtraining.com *"Charting the Course ... ... to Your Success!"*

Splunk Data Onboarding

Course Outline

I. Lookups
- A. Learn how to use lookups to add new fields to your events
- B. Go through a step by step example for creating a file-based/CSV lookup and search with the new lookup fields
- C. Configure a lookup to run automatically
- D. Learn about the lookup and inputlookup search commands to search and preview your lookup, respectively.
- E. Use outputlookup command to write search results to a lookup table

Lab: Configure an automatic lookup

II. Fields
- A. Use the fields sidebar to discover automatically extracted fields and view selected and interesting fields, add fields to your search.
- B. Walkthrough an example creating custom fields with props

Lab: Create search time fields using interactive field extractor or props

III. Props and Transforms
- A. Review key index time configuration in props to handle timestamp extractions, event breaking, (sourcetype, host, and source) assignments.
- B. Review search time operations:
  1. EXTRACT,REPORT, KV-MODE, FIELDALIAS, EVAL, and LOOKUP
- C. Configuration in props to handle timestamp extractions, event breaking, (sourcetype, host, and source) assignments.
- D. Describe different uses for transforms including
  1. Metadata rewrites
- E. For example mask sensitive data with SED command, dynamic sourcetype, host, source assignment at index time
- F. Best practices for onboarding data with props

Lab: Create props and transform configuration to index a sample data file

IV. Tags and Event Types
- A. Understand tags to categorize and add meaning to data.
- B. Understand Event types to group common events.
- C. Create tags and event types and use them in search

Lab: Create a tag and event type and use them in search

V. Workflow Actions
- A. Understand how workflow actions allow you to create custom actions for events and fields.
- B. Describe different examples for workflow actions including performing external IP lookup, launch secondary searches, perform external search.
- C. Walk through an example for configure workflow action in Splunk Web

Lab: Create a workflow action

VI. Alerts
- A. Understand how alerts are used in Splunk to timely updates on triggered conditions in your data
- B. Go through steps for configuring different types of alerts; pre-result alerts, scheduled alters, and rolling window alerts
- C. Overview on managing alerts including Managing alert permissions,

Lab: Create an alert and view fired alerts

Splunk Data Onboarding

Course Outline (cont'd)

VII. Scheduled Reports
- A. Understand how to schedule a report to run on a scheduled interval
- B. Describe different actions supported by Splunk when trigger conditions are met including send an email, run a script, write to a CSV lookup
- C. Go through steps for creating a scheduled in Splunk Web

Lab: Create and schedule your own report

VIII. Macros
- A. Understand how macros work as reusable chunks of SPL that can be inserted in other searches.
- B. Go through steps for creating a macro in Splunk Web
- C. Use a macro in a search

Lab: Create a macro to search index

IX. Data Models
- A. Review different data model concepts including root and child objects, constraints and attributes, object attributes.
- B. Walk through an example for using data model builder and Pivot UI.
- C. Use Pivots to search and create reports from data models.
- D. Describe how to accelerate a data model for faster reports.

Lab: Create a data model

X. Common Information Model
- A. Understand CIM for normalizing data in Splunk
- B. Overview of CIM app and the different data sets provided in the app

Lab: Explore different data sets in CIM app