SPLUNK POWER USER

STUDY MATERIALS

1. STUDY GUIDE
2. PRACTICE QUESTIONS
3. ZERO TO POWER USER COURSE
4. STEP TRAINING

1.0 Using Transforming Commands for Visualizations 5%

1.1 Use the chart command

- Returns results in a table format.
- Can create different charts

1.2 Use the timechart command

- Returns a time chart (Associates values with a time)
- Timeseries

2.0 Filtering and Formatting Results 10%

2.1 The eval command

- Does the math you ask
- Create new fields
- Converts data

2.2 Use the search and where commands to filter results

Search:

- Place anywhere in the SPL
- Search for a keyword or variable
- Seach with wildcards

Where:

- Comparing values “Show results where x equals…”
- Use with functions
- “” “” =field values

- ‘ ‘ =field names

2.3 The fillnull command

- If you don’t specify a value it will turn into 0
- Fillnull=value

3.0 Correlating Events 15%

3.1 Identify transactions

- Transaction is for turning multiple into 1 event
- It is also for things with a start/end time
- Use shared fields
-

3.2 Group events using fields

- Stats command
- Chart and timechart command
- Eval command for custom groupings

3.3 Group events using fields and time

- Use of the timecharrt command for grouping event by both time and fields
- Use the stats command to group events by fields and time. But you might have to use the bin command
- Transaction command is useful when events occur close to eachother in time
-

3.4 Search with transactions

- maxspan/maxpause
- startswith/endswith
- Use it for session tracking

3.5 Report on transactions

- Save search
- Schedule the report
- Export the resolds in CSV, JSON, or PDF

3.6 Determine when to use transactions vs. stats

- Stats when you need it to be fast and efficient
- Transactions when you have multiple events in a short amount of time

4.0 Creating and Managing Fields 10%

4.1 Perform regex field extractions using the Field Extractor (FX)

- Run a search
- Event actions
- Extract new fields
- Regular expression
- Assign a name with field name

4.2 Perform delimiter field extractions using the FX

- Run a search
- Event actions
- Extract new fields
- Delimited
- Specify the delimiter
- Assign a name with field name

5.0 Creating Field Aliases and Calculated Fields 10%

5.1 Describe, create, and use field aliases

- Field aliases replace values and are searchable after it is defined in search string

5.2 Describe, create, and use calculated fields

- Field that comes from other fields using expressions or formulas
- Settings>Fields>Calculated fields , select app,new calculated field, define field, save field

6.0 Creating Tags and Event Types 10%

6.1 Create and use tags

- Select actions beside the field value pair and then edit tags (it will show tag:: value)

6.2 Describe event types and their uses

- Event types are search strings saved to show a certain thing

6.3 Create an event type

- Run a search

- Save as event type
- Provide a name
- Then use the event type by searching for it

7.0 Creating and Using Macros 10%

7.1 Describe macros

- Saved off searches that can be used by running the name in the search bar
- It never changes unless you change it
- Surrounded by back ticks, not single quotes
- Saves time for running reports everyday

7.2 Create and use a basic macro

- settings>Advanced Search>Search macros
- Create new macro (name and definition)
- Save
- Use by surrounding it with back ticks (` `)

7.3 Define arguments and variables for a macro

- Define arguments in the arguments tab and the have the number of arguments at the end of the macro name in parenthesis
  Ex:loglevel(3)

7.4 Add and use arguments with a macro

- Pass the argument through the marco
  Ex:` `loglevel`(FAIL)`

8.0 Creating and Using Workflow Actions 10%

8.1 Describe the function of GET, POST, and Search workflow actions

- get=retrieve
- put=send
- search=secondarty search
- link.method= get

8.2 Create a GET workflow action

- Define link
- Define name
- Decide where to open link on a new window or same window
- link.method=post

8.3 Create a POST workflow action

- Define link
- Define argument

8.4 Create a Search workflow action

- Type =search , then set a specific setting to define secondary search with search.ear liest

9.0 Creating Data Models 10%

9.1 Describe the relationship between data models and pivot

- Pivot tool leverages data models to allow users to build tables, charts and reports without needing to write SPL
- Pivot creates a visualization of datamodels
- Datamodel can be a command or an argument. You can reference a data model by using (datamodel= (datamodel))

9.2 Identify data model attributes

- **Datasets**: These are subsets of events or objects. They can be hierarchically organized with parent-child relationships, where child datasets inherit fields from parent datasets.
- **Fields**: Data models use fields, which can be auto-extracted or created with **lookups**, **regex**, or **eval expressions**.
- **Constraints**: These define what data a dataset includes. For example, you can constrain a dataset to include only events with a particular `sourcetype` or `status_code`.
- **Calculated Fields**: These are fields generated dynamically at search time using expressions, often to create new insights or perform calculations.
- **Accelerated Data Models**: You can configure a data model to be accelerated for faster reporting and searches, which is especially useful for large datasets
  Splunk Documentation

  Splunk
  .

9.3 Create a data model

- Settings, datatmodels,new datamodel
- Define the datamodel
- Add datasets (sourcetypes= access_combined)

10.0 Using the Common Information Model (CIM) Add-On 10%

10.1 Describe the Splunk CIM

- Normalize data
- A model to use and reference
- An application (ADD on and Add on builder)

10.2 List the knowledge objects included with the Splunk CIM Add-On

- Preconfigured datamodels
- Fields and event category tags

- Alerts
- Authentication
- Email
- Databases
- Java Virtual Machines (JVM)
- Application State
- Malware
- Network Resolution (DNS)
- Certificates
- Network Sessions
- Change Analysis
- Network Traffic
- CIM Validation (S.o.S)
- Performance
- Splunk Audit Logs
- Ticket Management
- Interprocess Messaging
- Updates
- Intrusion Detection
- Vulnerabilities Inventory
- Web

10.3 Use the CIM Add-On to normalize data

-