Splunk Development Advance Level\_TOC

|  |  |  |  |
| --- | --- | --- | --- |
|  | | |  |
| **Day** | **Module** | **Topics** | **Duration** |
|  |  |  |  |
| **Day - 1** | **Introduction** | What is Splunk | 2 hrs. |
|  |  | How Splunk Started |  |
|  |  | Splunk Overview |  |
|  |  | Splunk Real Time Examples |  |
|  |  | Splunk Deployment Methods |  |
|  |  | Splunk Installation Lab |  |
|  |  |  |  |
|  | **Splunk Commands** | stats | 2 hrs. |
|  |  | field |  |
|  |  | table |  |
|  |  | rex |  |
|  |  | rename |  |
|  |  | where |  |
|  |  | top |  |
|  |  | rare |  |
|  |  | Join |  |
|  |  | addcoltotals |  |
|  |  | chart |  |
|  |  | timechart |  |
|  |  | Eventcount |  |
|  |  |  |  |
|  | **Using Transforming Commands**  **for Visualizations** | Use the chart command |  |
|  |  | Use the timechart comman |  |
|  |  |  |  |
|  | **Filtering and Formatting Results** | The eval command | 1 hrs. |
|  |  | Use the search and where commands to  filter results |  |
|  |  | The fillnull command |  |
|  |  |  |  |
|  | **Exploring Statistical Commands** | Performing statistical analysis with stats function | 1 hrs. |
|  |  | Using fieldsummary |  |
|  |  | Using appendpipe |  |
|  |  | Using count and list functions |  |
|  |  | Using eventstats |  |
|  |  | Using streamstats |  |
|  |  |  |  |
|  | **Exploring eval Command Functions** | conversion functions | 1 hrs. |
|  |  | text functions |  |
|  |  | comparison and conditional function |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | informational functions |  |  |
|  |  | statistical functions |  |  |
|  |  | makeresults command |  |  |
|  |  |  |  |  |
|  | Correlating Events | Identify transactions | 1 hr. |  |
|  |  | Group events using fields |  |  |
|  |  | Group events using fields and time |  |  |
|  |  | Search with transactions |  |  |
|  |  | Report on transactions |  |  |
|  |  | Determine when to use transactions vs. stats |  |  |
|  |  |  |  |  |
| Day - 2 | Exploring Lookups | Applying advanced lookup options | 3 hrs. |  |
|  |  | Including and excluding events  based on lookup values |  |  |
|  |  | Using KV Store lookups |  |  |
|  |  | Using external lookups |  |  |
|  |  | Using geospatial lookups |  |  |
|  |  | Understanding best practices for lookups |  |  |
|  |  |  |  |  |
|  | Exploring Alerts | Logging and indexing searchable alert events | 1 hrs. |  |
|  |  | Referencing lookups in alerts |  |  |
|  |  | Outputting alert results to a lookup |  |  |
|  |  | Using a webhook alert action |  |  |
|  |  | Creating a log event alert action |  |  |
|  |  |  |  |  |
|  | Creating and Managing Fields | Perform regex field extractions  using the Field Extractor | 2 hrs. |  |
|  |  | Perform delimiter field extractions  using the FX |  |  |
|  |  | Identifying field extraction methods |  |  |
|  |  | Providing a regex expression to the Field Extractor to |  |  |
|  |  | Performing search time field extraction  using the erex |  |  |
|  |  | mands |  |  |
|  |  | Understand how to improve regex  performance in Splunk |  |  |
|  |  |  |  |  |
|  | Working with Self-Describing Data and Files | Understanding self-describing data | 1 hrs. |  |
|  |  | Using the spath command |  |  |
|  |  | Using the eval command with the spath function |  |  |
|  |  | Using the multikv command |  |  |
|  |  |  |  |  |
|  | Creating Field Aliases and Calculated Fields | Describe, create, and use field aliases | 1hrs. |  |
|  |  | Describe, create, and use calculated fields |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| Day - 3 | Creating Tags and Event Type | Create and use tags | 1 hr. |  |
|  |  | Describe event types and their uses |  |  |
|  |  | Create an event type |  |  |
|  |  |  |  |  |
|  | Creating and Using Macros | Describe macros | 1 hr. |  |
|  |  | Create and use a basic macro |  |  |
|  |  | Define arguments and variables for a macro |  |  |
|  |  | Add and use arguments with a macro |  |  |
|  |  | Using nested search macros |  |  |
|  |  | Previewing search macros before executing |  |  |
|  |  | Using other knowledge objects with macros |  |  |
|  |  |  |  |  |
|  | Creating and Using Workflow Actions | Describe the function of GET, POST, and Search workflow actions | 1 hr. |  |
|  |  | Create a GET workflow action |  |  |
|  |  | Create a POST workflow action |  |  |
|  |  | Create a Search workflow action |  |  |
|  |  |  |  |  |
|  | Creating Data Model | Describe the relationship between data models and pivot | 3 hrs. |  |
|  |  | Identify data model attributes |  |  |
|  |  | Create a data model |  |  |
|  |  | Exploring data models using the datamodel command |  |  |
|  |  | Understanding data model acceleration |  |  |
|  |  | Accelerating data models |  |  |
|  |  | Understanding tsidx files |  |  |
|  |  | Working with tsidx files using tstats commands |  |  |
|  |  | Using tstats to search accelerated data models |  |  |
|  |  | Determining which acceleration option to use |  |  |
|  |  |  |  |  |
|  | Using Acceleration Options: Reports and Summary Indexing | Describing acceleration | 2 hrs. |  |
|  |  | Identifying which reports qualify for acceleration |  |  |
|  |  | Identifying when Splunk doesn’t build an acceleration summary |  |  |
|  |  | Accelerating a report |  |  |
|  |  | Using the Report Acceleration Summaries and  Summary Detail pages |  |  |
|  |  | Understanding summary Indexing |  |  |
|  |  | Using the summary indexing transforming commands |  |  |
|  |  | Defining searching against a summary |  |  |
|  |  | Understanding how to handle gaps and overlaps in summary indexes |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| Day - 4 | Using Acceleration Options: Data Models and tsidx Files | Exploring data models using the datamodel command | 2 hrs. |  |
|  |  | Understanding data model acceleration |  |  |
|  |  | Accelerating data models |  |  |
|  |  | Understanding tsidx files |  |  |
|  |  | Working with tsidx files using tstats commands |  |  |
|  |  | Using tstats to search accelerated data models |  |  |
|  |  | Determining which acceleration option to use |  |  |
|  |  |  |  |  |
|  | Using Search Efficiently | Splunk architecture components | 1 hrs. |  |
|  |  | Search flow |  |  |
|  |  | Streaming commands |  |  |
|  |  | Transforming commands |  |  |
|  |  | Command ordering |  |  |
|  |  | Job inspector |  |  |
|  |  |  |  |  |
|  | More Search Tuning | Pre-Filtering search data | 1 hrs. |  |
|  |  | Lispy and boolean operators |  |  |
|  |  | Lispy and wildcards |  |  |
|  |  | Using the TERM directive |  |  |
|  |  |  |  |  |
|  | Manipulating and FIltering Data | bin command | 1.5 hrs. |  |
|  |  | xyseries command |  |  |
|  |  | untable command |  |  |
|  |  | foreach command |  |  |
|  |  | strftime function |  |  |
|  |  |  |  |  |
|  | Working with Multivalued Fields | Multivalued fields | 2.5 hrs. |  |
|  |  | Some multivalued eval functions |  |  |
|  |  | makemv command |  |  |
|  |  | mvexpand command |  |  |
|  |  |  |  |  |
| Day - 5 | Using Advanced Transactions | Evaluating events to create transactions | 3 hrs. |  |
|  |  | Handling common values/different field names |  |  |
|  |  | An alternative to coalesce |  |  |
|  |  | Identifying complete vs. incomplete transactions |  |  |
|  |  | Making transactions more efficient |  |  |
|  |  | stats and transactions | 0.5 hrs. |  |
|  |  |  |  |  |
|  | Working with Time | Using time effectively | 1 hrs. |  |
|  |  | What are the default time fields |  |  |
|  |  |  |  |  |
|  | Using Subsearches | Filtering through many results | 1.5 hrs. |  |
|  |  | Subsearch caveats |  |  |
|  |  | When to use subsearch |  |  |
|  |  | When NOT to use subsearch |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Troubleshooting subsearches |  |  |
|  |  | append command |  |  |
|  |  |  |  |  |
|  | Creating a Prototype | Define simple XML syntax for views | 2 hrs. |  |
|  |  | Use best practices for creating views |  |  |
|  |  | Troubleshooting views |  |  |
|  |  |  |  |  |
| Day - 6 | Using Forms | Explain how tokens work | 1.5 hrs. |  |
|  |  | Use tokens with form inputs |  |  |
|  |  | Create cascading inputs |  |  |
|  |  | Define types of token filters |  |  |
|  |  |  |  |  |
|  | Improving Performance | Identify ways to improve dashboard  Performance using base search, saved search and summary index | 2 hrs. |  |
|  |  | Use the tstats command | 0.5 hrs. |  |
|  |  | Create base and post-process searches |  |  |
|  |  |  |  |  |
|  | Customizing Dashboards | Customize chart and panel properties | 2 hrs. |  |
|  |  | Set panel refresh and delay times |  |  |
|  |  | Disable search access features |  |  |
|  |  | Create event annotations |  |  |
|  |  |  |  |  |
|  | Adding Drilldowns | Define types of drilldowns | 1 hrs. |  |
|  |  | Identify predefined tokens |  |  |
|  |  | Create dynamic drilldowns |  |  |
|  |  |  |  |  |
|  | Adding Advanced Behaviors  and Visualizations | Identify types of event handlers | 0.5 hrs. |  |
|  |  | Define event actions |  |  |
|  |  | Create contextual drilldowns |  |  |
|  |  | Use simple XML extensions |  |  |
|  |  |  |  |  |
|  | Splunk MLTK toolkit | Installation of Splunk MLTK | 0.5 hrs. |  |
|  |  | Implementation of Linear Regression |  |  |
|  |  | Deep dive into Splunk MLTK Commands |  |  |
|  |  |  |  |  |