

Splunk Basics

Module 1 – Exploring Statistical Commands

Performing statistical analysis with functions of the stat command

Using fieldsummary

Using appendpipe

Using eventstats

Using streamstats

Module 2 – Exploring eval Command Functions

Using conversion functions

Using data and time functions

Using string functions

Using comparison and conditional functions

Using informational functions

Using statistical functions

Using mathematical functions

Using cryptographic functions

Module 3 – Exploring Lookups

Including and excluding events based on lookup values

Using KV Store lookups

Using external lookups

Using geospatial lookups

Using database lookups

Understanding best practices for lookups

Module 4 – Exploring Alerts

Referencing lookups in alerts

Outputting alert results to a lookup

Logging and indexing searchable alert events

Using a webhook alert action

Module 5 – Advanced Field Creation and Management

Using regex

Using the erex command

Using the rex command

Identifying regex best practices

Module 6 – Working with Self-Describing Data and Files

Using the spath command

Using the eval command with the spath function

Extracting fields from table-formatted events with multikv

Module 7 – Advanced Search Macros

Using nested search macros

Previewing search macros before executing

Using tags and event types in search macros

Module 8 – Using Acceleration Options: Reports and Summary Indexing

Using report acceleration

Using summary indexing

Module 9 – Using Acceleration Options: Data Models and tsidx Files

Exploring data models using the datamodel command

Using data model acceleration

Working with tsidx files using the tstats command