

Splunk for Security Analysts

SEC405

Learn Splunk's Search Processing Language from your first search to mastery, against a month of security data with real attacks in it: searching and filtering, shaping, statistics, combining sources, text and multivalue data, macros and knowledge objects, time and sequence, data models with tstats, and the checks that keep searches fast and answers right.

Modules	21
Lessons	130
Phases	5
Free preview	Course Orientation (8 lessons)

The method

Every search runs in the page. A practice lab built into each lesson holds the sample month in eleven indexes with real sourcetype names and fields, five lookup tables and seven data models. Change a search, run it, and see what changed.

Predict, then run. Many searches ask for your prediction before they show their result, so every search is a small test of your understanding.

Three exercises in every lesson. Complete a search, fix a broken one, and write one from a blank editor, each graded on the result it returns. Each module ends with a knowledge check and a challenge set of questions the lessons did not answer.

Check every answer. The course treats an empty result, a round number and a borrowed, published or AI-written search as things to verify before anyone relies on them, and teaches the checks that do it.

Full syllabus

Orientation

Course Orientation [FREE PREVIEW](#)

Splunk for Security Analysts: Splunk's Search Processing Language, taught against one month of an engineering company's events with several real attacks in them.

1. 0.1 What SPL Is and Where It Runs
2. 0.2 How Splunk Stores Events
3. 0.3 The Sourcetypes a Security Analyst Searches
4. 0.4 Splunk Enterprise, Splunk Cloud Platform and SPL2
5. 0.5 Your First Search
6. 0.6 The Practice Lab and the Sample Month
7. 0.7 How to Learn SPL: the Mastery Ladder
8. 0.8 What This Course Builds

Foundation

Search Structure and Fields

Module 1 of Splunk for Security Analysts: how a question becomes an SPL search, the search pipeline and command order, learning an unfamiliar sourcetype, field values and types, missing fields, checking a result, and reading a search you did not write.

1. 1.1 Turning a Question into SPL
2. 1.2 The Search Pipeline
3. 1.3 Command Order and Command Types
4. 1.4 Learning a Sourcetype You Have Never Seen
5. 1.5 Field Values and Types
6. 1.6 Missing Fields and Nulls
7. 1.7 Checking a Result Against Its Events
8. 1.8 Reading a Search You Did Not Write
9. Module Summary and Knowledge Check

Searching and Filtering

Module 2 of Splunk for Security Analysts: how the base search chooses events.

1. 2.1 Search Terms and the Index
2. 2.2 Field Values and Boolean Logic
3. 2.3 Wildcards and Matching
4. 2.4 Time Ranges and Time Modifiers
5. 2.5 search Versus where
6. 2.6 Addresses and CIDR
7. 2.7 Fields Inside JSON
8. 2.8 Negative Filters
9. Module Summary and Knowledge Check

Shaping Results

Module 3 of Splunk for Security Analysts: what a search does with the events it chose.

1. 3.1 eval Expressions
2. 3.2 if, case and Labels
3. 3.3 Text Functions
4. 3.4 Time Formats
5. 3.5 table, fields and rename
6. 3.6 sort, head and tail
7. 3.7 dedup
8. 3.8 Presenting a Result
9. Module Summary and Knowledge Check

Intermediate

Statistics

Module 4 of Splunk for Security Analysts: summarizing events into numbers that mean something.

1. 4.1 The stats Command
2. 4.2 Counting Correctly
3. 4.3 Distributions and Percentiles
4. 4.4 Conditional Statistics
5. 4.5 values and list
6. 4.6 timechart
7. 4.7 chart, xyseries and untable
8. 4.8 Rates and the Averages That Mislead
9. Module Summary and Knowledge Check

Combining Data

Module 5 of Splunk for Security Analysts: bringing data together.

1. 5.1 Lookups
2. 5.2 inputlookup and Lookup Tables
3. 5.3 Subsearches and Their Limits
4. 5.4 join and Its Limits
5. 5.5 append and appendcols
6. 5.6 multisearch and union
7. 5.7 Correlating with stats
8. 5.8 Correlating Across Time
9. Module Summary and Knowledge Check

Text and Multivalue Data

Module 6 of Splunk for Security Analysts: working inside fields.

1. 6.1 rex
2. 6.2 rex in sed Mode and the regex Command
3. 6.3 spath and JSON
4. 6.4 Multivalue Fields
5. 6.5 makemv, split and mvexpand
6. 6.6 Multivalue Functions
7. 6.7 Key-Value Data
8. 6.8 Decoding
9. Module Summary and Knowledge Check

Advanced

Macros, Lookups and Knowledge Objects

Module 7 of Splunk for Security Analysts: logic written once and used everywhere.

1. 7.1 Search Macros
2. 7.2 Macros with Arguments
3. 7.3 Lookup Definitions
4. 7.4 Field Aliases and Calculated Fields
5. 7.5 Event Types and Tags
6. 7.6 Saved Searches
7. 7.7 foreach
8. 7.8 Reusable eval Patterns
9. Module Summary and Knowledge Check

Time and Sequence

Module 8 of Splunk for Security Analysts: events in time.

1. 8.1 bin and span
2. 8.2 Comparing Periods
3. 8.3 eventstats Baselines
4. 8.4 streamstats Windows
5. 8.5 delta and the Previous Event
6. 8.6 transaction and Sessions
7. 8.7 First and Last per Entity
8. 8.8 Running Totals
9. Module Summary and Knowledge Check

Data Models and tstats

Module 9 of Splunk for Security Analysts: the Common Information Model, data models and datasets, the datamodel command, tstats, summariesonly and acceleration, tstats with by and where, rewriting raw searches for data models, and checking when a data model answers differently.

1. 9.1 The Common Information Model
2. 9.2 Data Models and Datasets
3. 9.3 The datamodel Command
4. 9.4 tstats
5. 9.5 summariesonly and Acceleration
6. 9.6 tstats with by and where
7. 9.7 From Raw Search to Data Model Search
8. 9.8 When a Data Model Answers Differently
9. Module Summary and Knowledge Check

Mastery

Search Optimization and Validation

Module 10 of Splunk for Security Analysts: how a search runs, filtering first, command types and placement, transforming early, limits and truncation, reading and adapting public searches, checking the answer, checking AI-written SPL, and from SPL to SPL2.

1. 10.1 How a Search Runs
2. 10.2 Filter First
3. 10.3 Command Types and Placement
4. 10.4 Transforming Early
5. 10.5 Limits and Truncation
6. 10.6 Reading and Adapting Public Searches
7. 10.7 Checking the Answer
8. 10.8 Checking AI-Written SPL
9. 10.9 From SPL to SPL2
10. Module Summary and Knowledge Check

Phase 0: Course Resources

Cheatsheets

One sheet per module of Splunk for Security Analysts, each entry a question, a search that answers it against the sample month, what to read and what the answer does not prove.

1. Sources and the Lab
2. Search Structure and Fields
3. Searching and Filtering
4. Shaping Results
5. Statistics
6. Combining Data
7. Text and Multivalue Data
8. Macros, Lookups and Knowledge Objects
9. Time and Sequence
10. Data Models and tstats
11. Optimization and Validation

Cookbooks

Procedures for the problems every SPL user meets: a search that returns nothing, a search that is too slow, and a source nobody has searched before.

1. A Search Returns Nothing
2. A Search Is Too Slow
3. Taking Apart an Unfamiliar Source

Lab Setup

The practice lab the course runs in, and how to get a Splunk of your own for the Project: an employer's deployment, Splunk Enterprise on its trial or Free license, or a Splunk Cloud Platform trial.

1. The Practice Lab
2. Your Own Splunk

Walkthroughs

Six searches from the course that ran cleanly and answered wrongly, each taken step by step to the right answer: a sort's limit, an early head, a missing field, a silent detection, a lookup's default and a ranking.

1. The Month That Was Twelve Days
2. The Answer About Four Days
3. The Field That Was Not There
4. The Detection That Never Fired
5. The Country Everyone Came From
6. The Exfiltration That Ranked Third

Search Patterns

Six search patterns analysts reuse: first time seen, rare in the population, volume against its own normal, many accounts from one source, regular gaps, and success after failures.

1. First Time Seen
2. Rare in the Population
3. Volume Against Its Own Normal
4. Many Accounts From One Source
5. Regular Gaps
6. Success After Failures

Playground

Resources for practicing SPL and using it at work: a free-run search console, two guided SPL drills, the detection library, response playbooks, and an open-source DFIR toolkit.

Operational Reference

Every command, function, check and limit from Splunk for Security Analysts in one place, organized by the task in front of you and linked back to the section that explains it.

1. Operational Reference

References & Further Reading

The documentation behind Splunk for Security Analysts, arranged by the question it answers: the language, where searches run and their limits, getting a Splunk to practice on, and published detections.

Project

Project: Your Own Search Library

The Splunk for Security Analysts project: a brief for a library of twenty searches you build on your own Splunk data, each answering a stated question, each checked, with its source's pitfalls and its cost noted, and one taken to the quality of a scheduled search.

1. The Brief

Course Completion

Course Exam

Splunk for Security Analysts end-of-course exam: twenty tasks, two per teaching module, each answered by writing SPL against the course's sample month and checked on the server.

1. Course Completion. Splunk for Security Analysts

Generated 2026-10-03 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/splunk-for-security-analysts/