Splunk 101 Hands-on Workshop

splunk>

Forward-looking statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Splunk 101 Session Overview

Session Goals:

- Enable your teams to search, investigate, analyze, & report on data
- Drive more value and better outcomes from machine data
- Increase teams' productivity and efficiency in resolving issues

Splunk 101 Agenda:

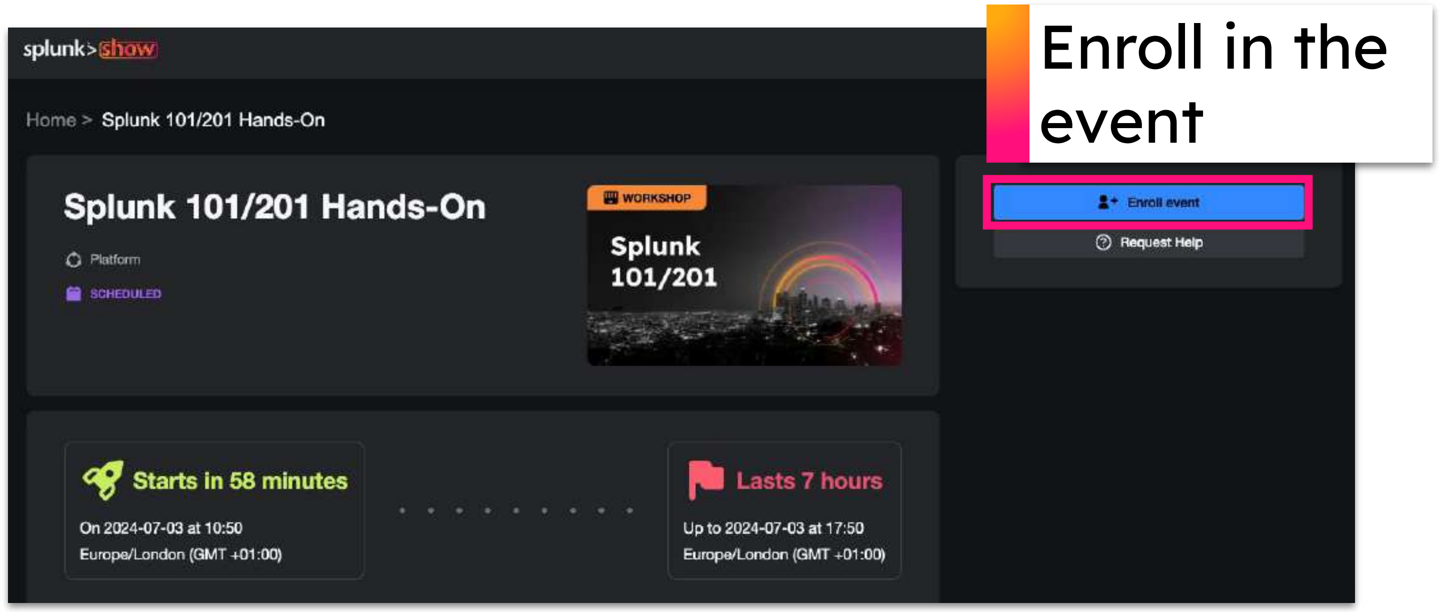
- Search UI (review)
- Anatomy of a Search & Best Practices (review)
- Popular SPL Commands
  - Top 4 Commands: stats, timechart, eval, where
  - Other Useful Commands: rename, table, dedup, fields, head/tail, top/rare
- Common Use Cases: Security, IT, and Observability

Lab Instance Enrollment & Log In

Tasks

1. Get a splunk.com account if you don't have one yet: https://splk.it/SignUp
2. Enroll in the Splunk Show workshop event: https://show.splunk.com/event/<eventID>
3. Download today's slides: https://splk.it/101-Attendee
4. Download the lab guide: https://splk.it/101-Lab-Guide
5. Download a copy of the Splunk Quick Reference Guide: https://splk.it/SplunkQuickRef

Goal



Splunk 101/201 Hands-On

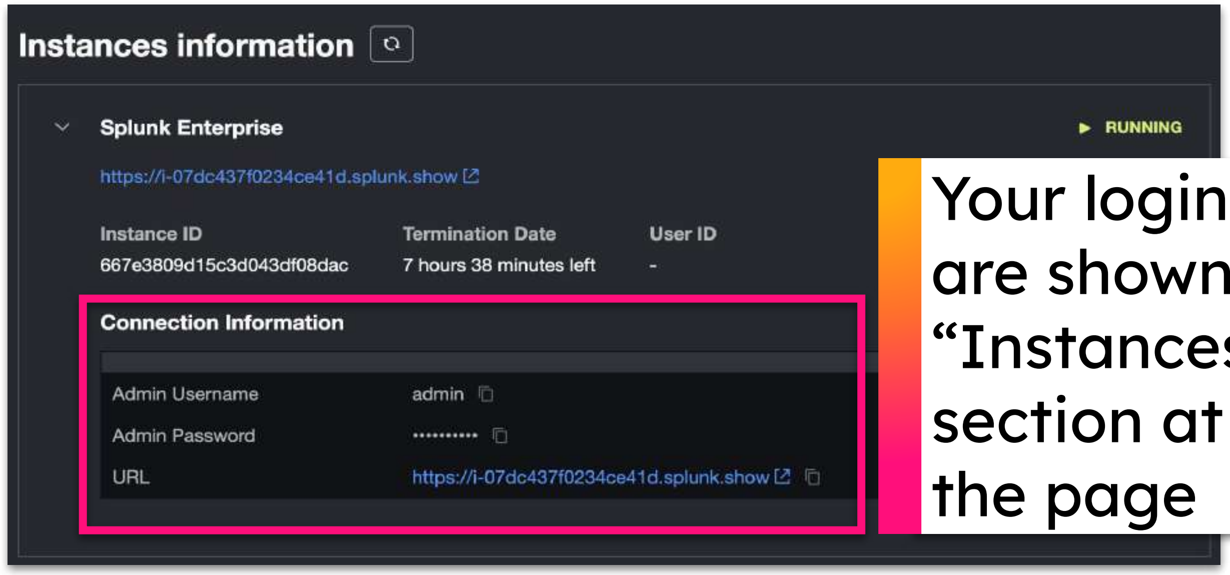
Platform

SCHEDULED

Starts in 58 minutes
On 2024-07-03 at 10:50
Europe/London (GMT +01:00)

Lasts 7 hours
Up to 2024-07-03 at 17:50
Europe/London (GMT +01:00)

Enroll in the event



Instances information

Splunk Enterprise

https://i-07dc437f0234ce41d.splunk.show

Instance ID	Termination Date	User ID
667e3809d15c3d043df08dac	7 hours 38 minutes left	-

Connection Information

Admin Username	admin
Admin Password	••••••••••
URL	https://i-07dc437f0234ce41d.splunk.show

Your login credentials are shown under the "Instances Information" section at the bottom of the page

Introduction

Splunk UI & Anatomy of an SPL Search

splunk>

Search UI

Search & investigate logs for errors:

- `sourcetype=* error`

Quick reports:

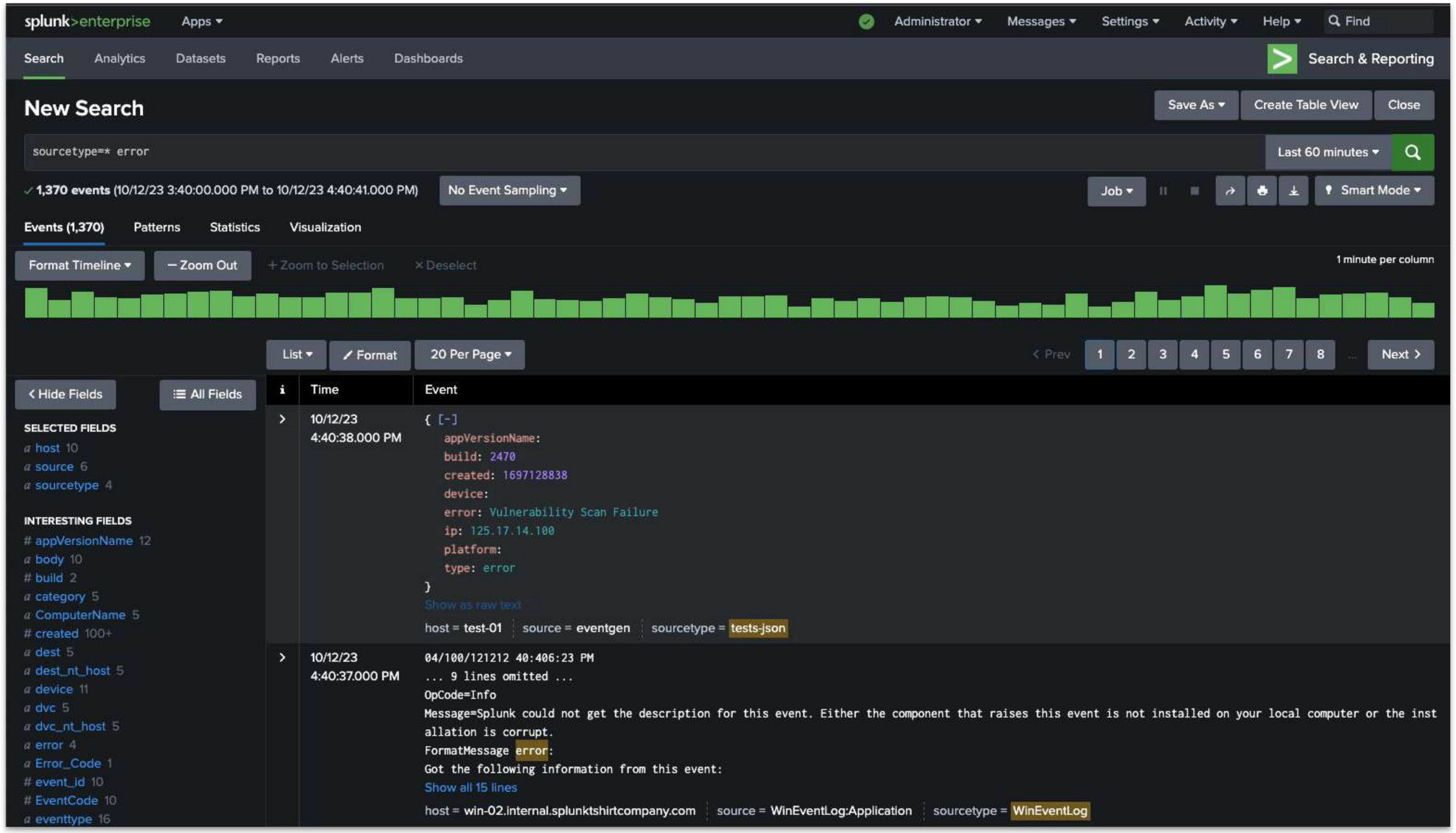
- Top values (by time), rare values
- Events with this field
- Average/Maximum/Minimum over time

Customize time spans

- Relative, Real-time, Date & Time Range

Outcomes & value:

- Find needle-in-haystack problems or threats
- Reduce Mean Time To Resolve (MTTR) issues



```
sourcetype=* error
```

✓ 1,370 events (10/12/23 3:40:00.000 PM to 10/12/23 4:40:41.000 PM)

SELECTED FIELDS

- a host 10
- a source 6
- a sourcetype 4

INTERESTING FIELDS

- # appVersionName 12
- a body 10
- # build 2
- a category 5
- a ComputerName 5
- # created 100+
- a dest 5
- a dest_nt_host 5
- a device 11
- a dvc 5
- a dvc_nt_host 5
- a error 4
- a Error_Code 1
- # event_id 10
- # EventCode 10
- a eventtype 16

10/12/23 4:40:38.000 PM

```
{ [-]
   appVersionName:
   build: 2470
   created: 1697128838
   device:
   error: Vulnerability Scan Failure
   ip: 125.17.14.100
   platform:
   type: error
}
```

Show as raw text

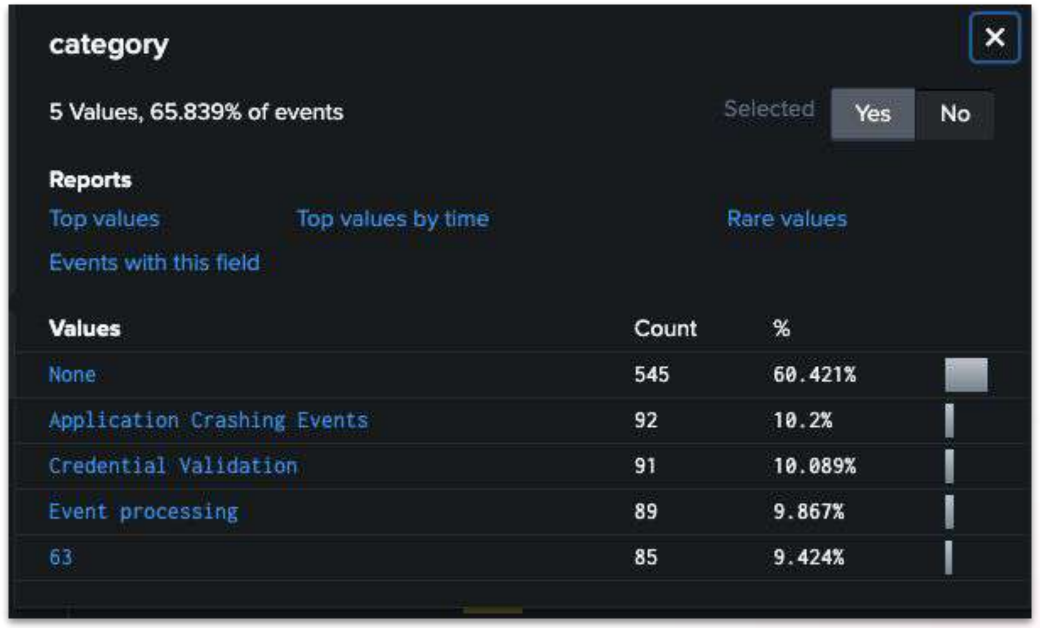
host = test-01 | source = eventgen | sourcetype = tests-json

10/12/23 4:40:37.000 PM

```
04/100/121212 40:406:23 PM
... 9 lines omitted ...
OpCode=Info
Message=Splunk could not get the description for this event. Either the component that raises this event is not installed on your local computer or the inst
allation is corrupt.
FormatMessage error:
Got the following information from this event:
```

Show all 15 lines

host = win-02.internal.splunktshirtcompany.com | source = WinEventLog:Application | sourcetype = WinEventLog



category

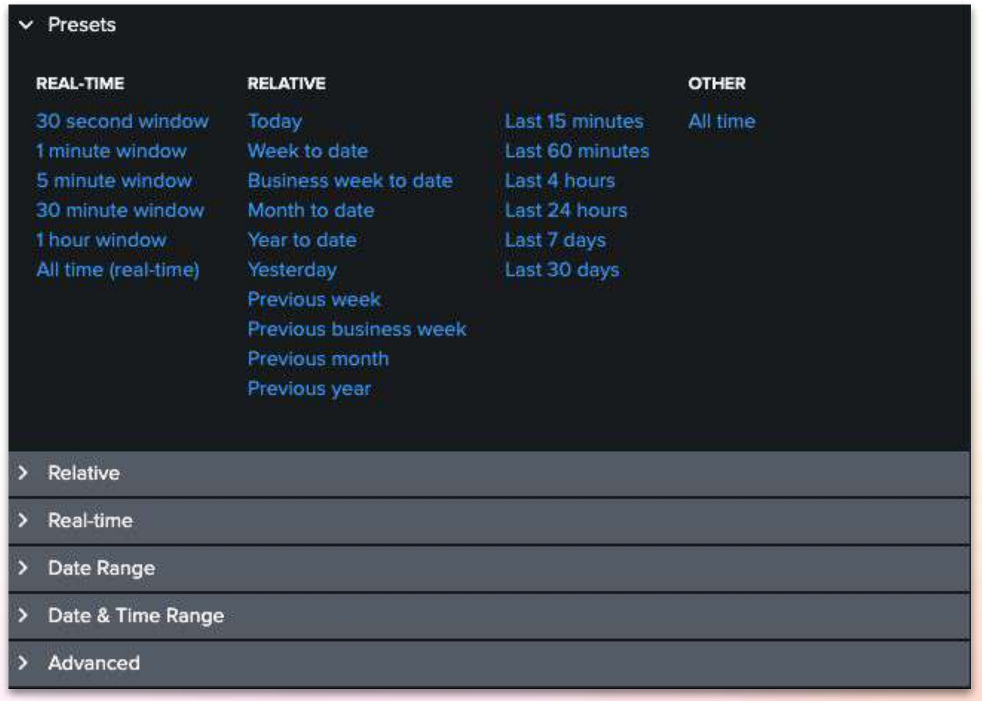
5 Values, 65.839% of events

Reports

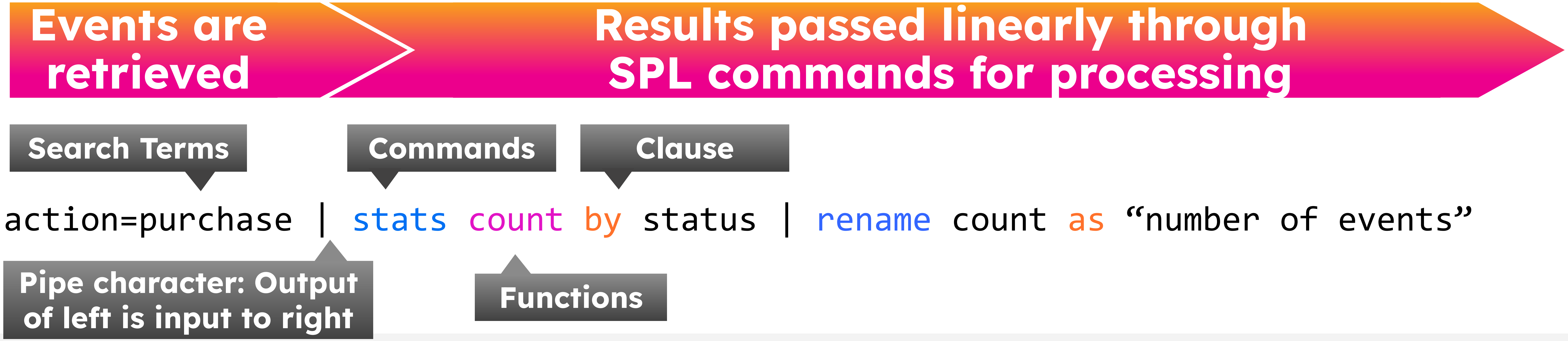
Top values | Top values by time | Rare values

Events with this field

Values	Count	%
None	545	60.421%
Application Crashing Events	92	10.2%
Credential Validation	91	10.089%
Event processing	89	9.867%
63	85	9.424%



SPL (Search Processing Language) Refresher



Events are retrieved

Results passed linearly through SPL commands for processing

Search Terms

Commands

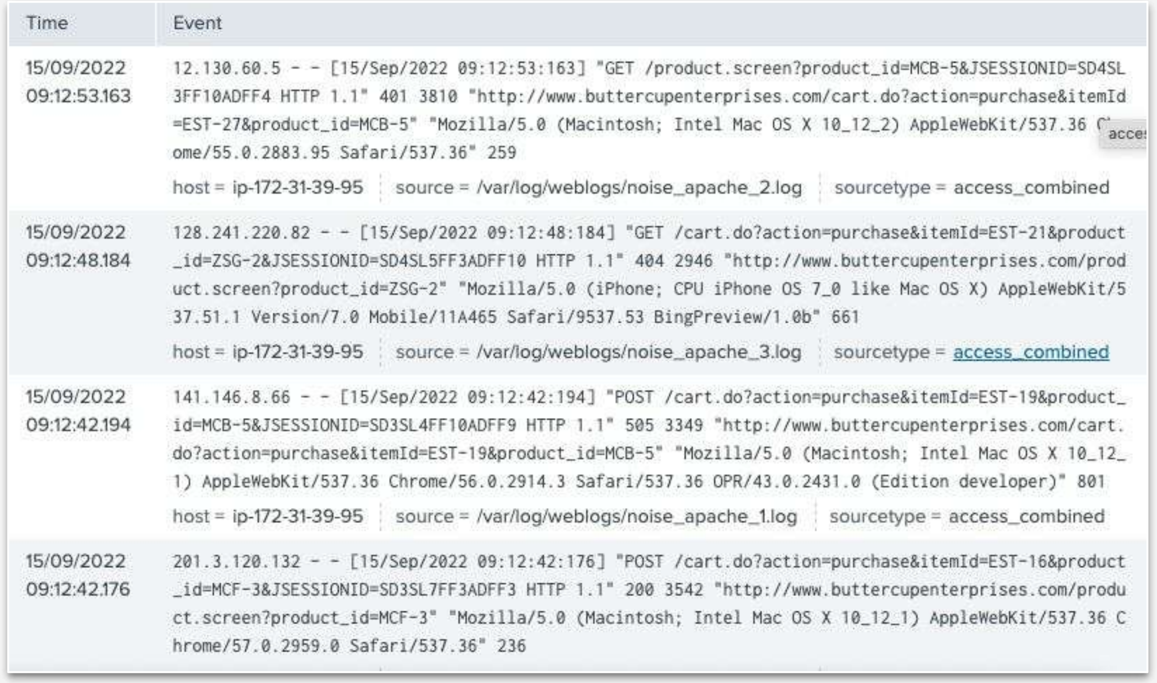
Clause

```
action=purchase | stats count by status | rename count as “number of events”
```

Pipe character: Output of left is input to right

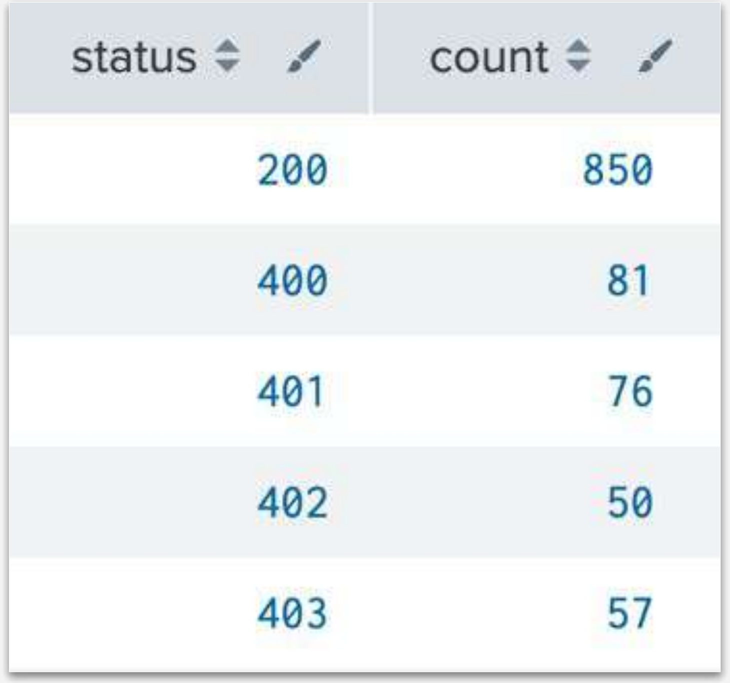
Functions

```
action=purchase
```



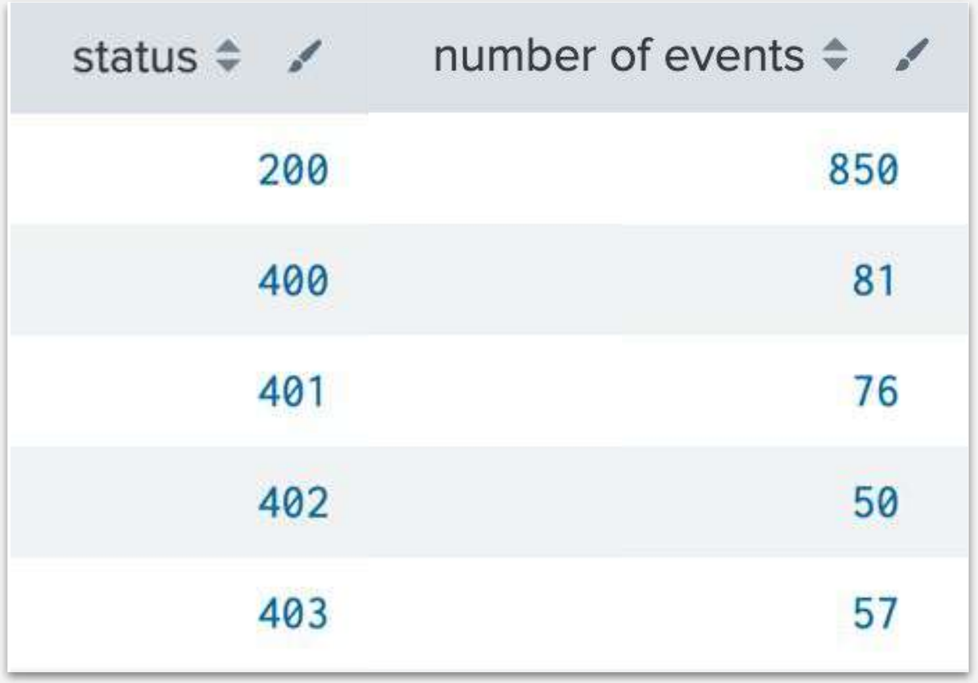
Time	Event
15/09/2022 09:12:53.163	12.130.60.5 - - [15/Sep/2022 09:12:53:163] "GET /product.screen?product_id=MCB-5&JSESSIONID=SD4SL3FF10ADFF4 HTTP 1.1" 401 3810 "http://www.buttercupenterprises.com/cart.do?action=purchase&itemId=EST-27&product_id=MCB-5" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_2) AppleWebKit/537.36 C ome/55.0.2883.95 Safari/537.36" 259 host = ip-172-31-39-95 ⋮ source = /var/log/weblogs/noise_apache_2.log ⋮ sourcetype = access_combined
15/09/2022 09:12:48.184	128.241.220.82 - - [15/Sep/2022 09:12:48:184] "GET /cart.do?action=purchase&itemId=EST-21&product_id=ZSG-2&JSESSIONID=SD4SL5FF3ADFF10 HTTP 1.1" 404 2946 "http://www.buttercupenterprises.com/product.screen?product_id=ZSG-2" "Mozilla/5.0 (iPhone; CPU iPhone OS 7_0 like Mac OS X) AppleWebKit/537.51.1 Version/7.0 Mobile/11A465 Safari/9537.53 BingPreview/1.0b" 661 host = ip-172-31-39-95 ⋮ source = /var/log/weblogs/noise_apache_3.log ⋮ sourcetype = access_combined
15/09/2022 09:12:42.194	141.146.8.66 - - [15/Sep/2022 09:12:42:194] "POST /cart.do?action=purchase&itemId=EST-19&product_id=MCB-5&JSESSIONID=SD3SL4FF10ADFF9 HTTP 1.1" 505 3349 "http://www.buttercupenterprises.com/cart.do?action=purchase&itemId=EST-19&product_id=MCB-5" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_1) AppleWebKit/537.36 Chrome/56.0.2914.3 Safari/537.36 OPR/43.0.2431.0 (Edition developer)" 801 host = ip-172-31-39-95 ⋮ source = /var/log/weblogs/noise_apache_1.log ⋮ sourcetype = access_combined
15/09/2022 09:12:42.176	201.3.120.132 - - [15/Sep/2022 09:12:42:176] "POST /cart.do?action=purchase&itemId=EST-16&product_id=MCF-3&JSESSIONID=SD3SL7FF3ADFF3 HTTP 1.1" 200 3542 "http://www.buttercupenterprises.com/product.screen?product_id=MCF-3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_1) AppleWebKit/537.36 Chrome/57.0.2959.0 Safari/537.36" 236

```
| stats count by status
```



status	count
200	850
400	81
401	76
402	50
403	57

```
| rename count as “number of events”
```



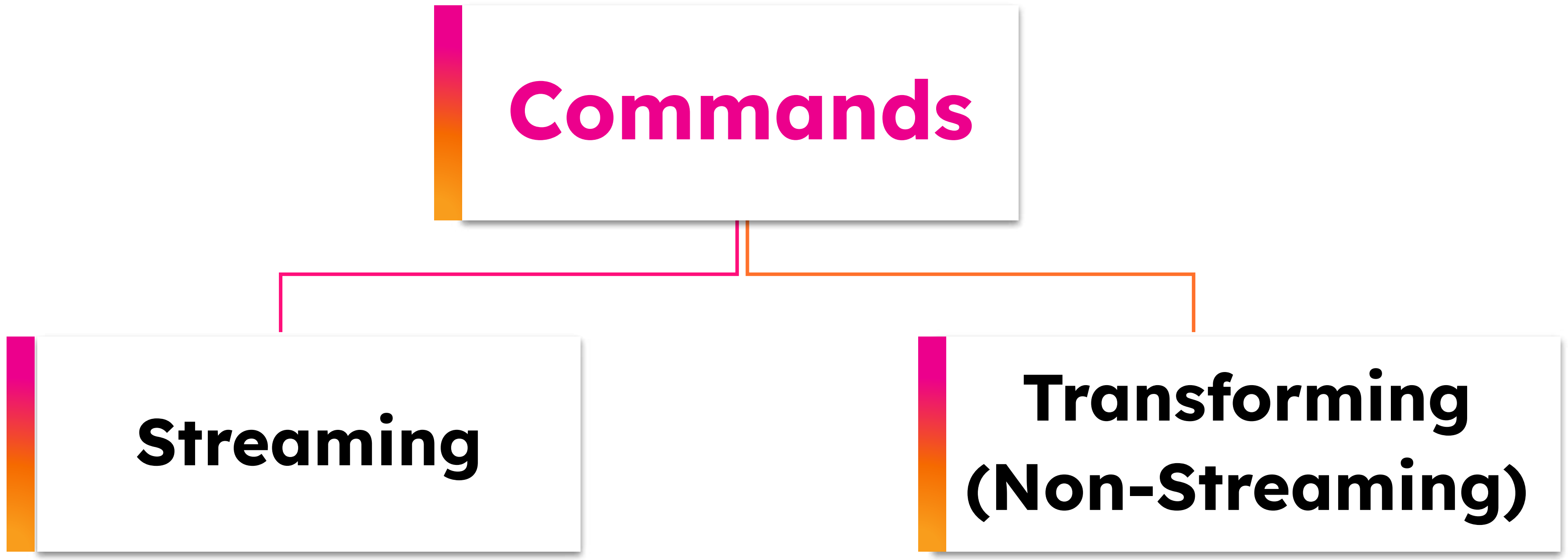
status	number of events
200	850
400	81
401	76
402	50
403	57

Want to know more? Check out:

Splunk Quick Reference Guide: https://splk.it/SplunkQuickRef

Search Manual: https://splk.it/SplunkSearchManual

Streaming & Transforming Commands



Commands

Streaming

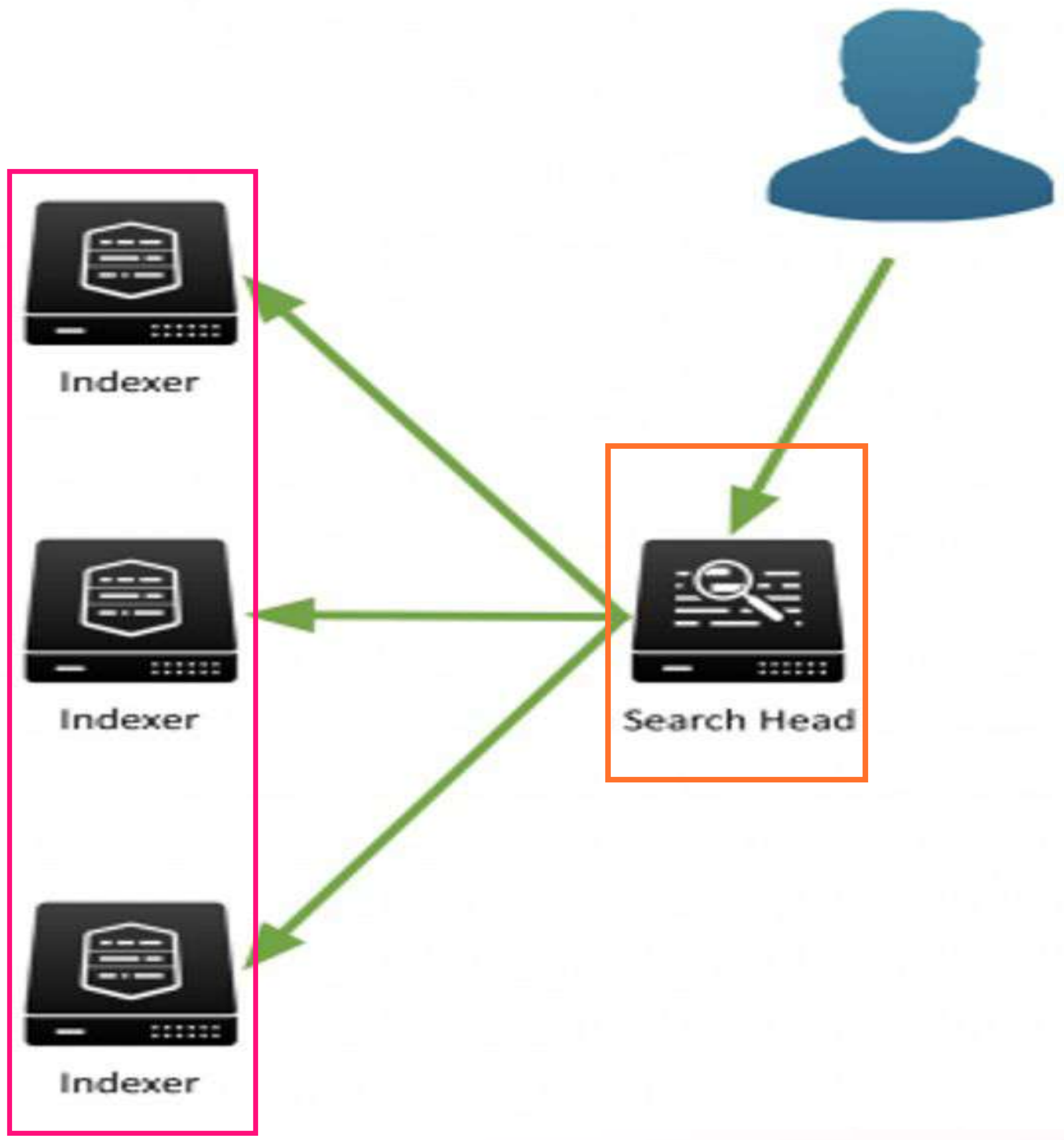
Transforming (Non-Streaming)

Streaming Commands

- Runs on the **indexers**
- Can be applied to subsets of index data in ***parallel***

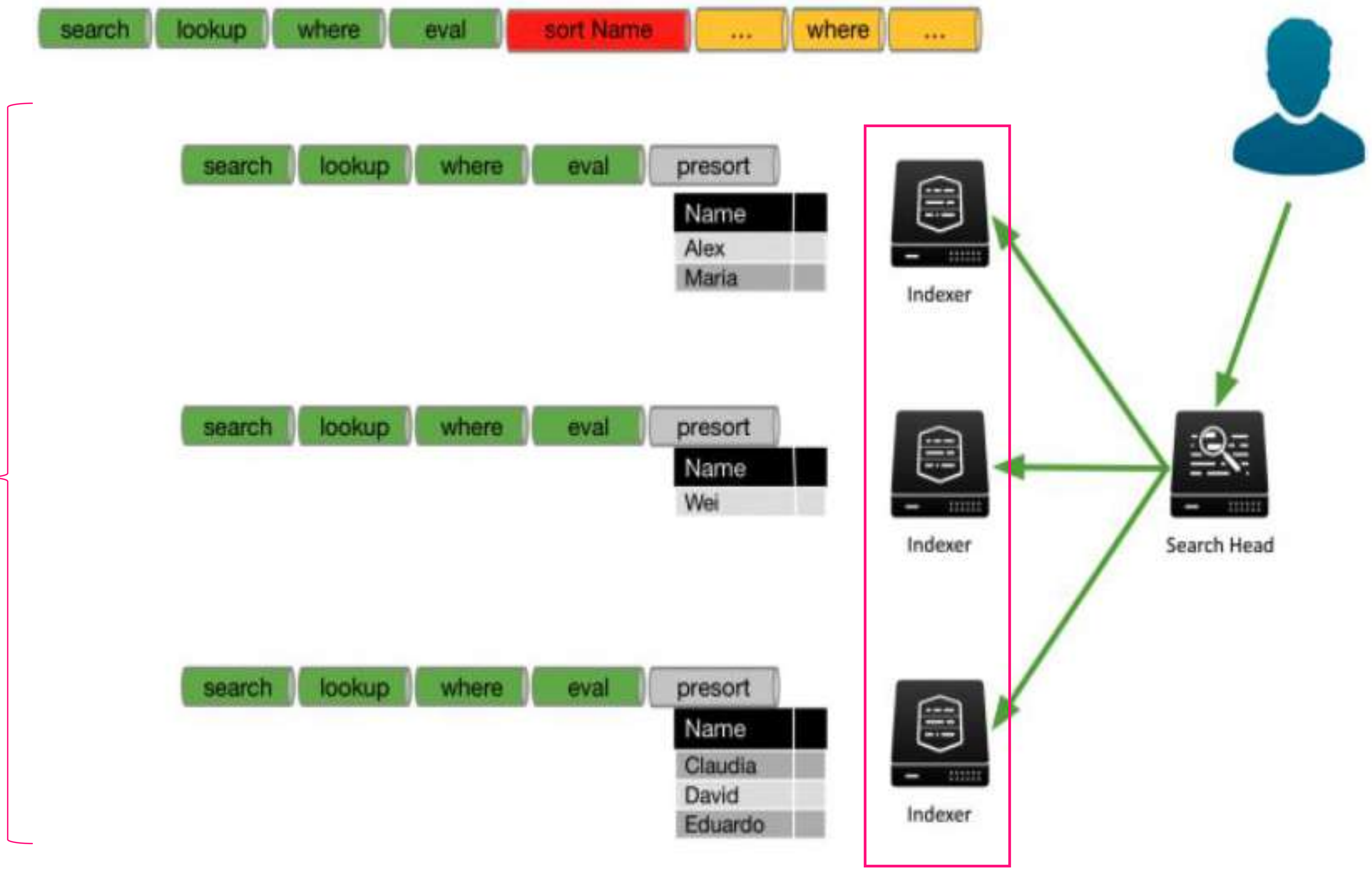
Transforming Commands

- Runs on the **Search Head**
- **Requires the events from all of the indexers** before the command can operate on the entire set of events.



Search Processing Example

Executed on Indexers



search | lookup | where | eval | sort Name | ... | where | ...

search | lookup | where | eval | presort

Name
Alex
Maria

search | lookup | where | eval | presort

Name
Wei

search | lookup | where | eval | presort

Name
Claudia
David
Eduardo

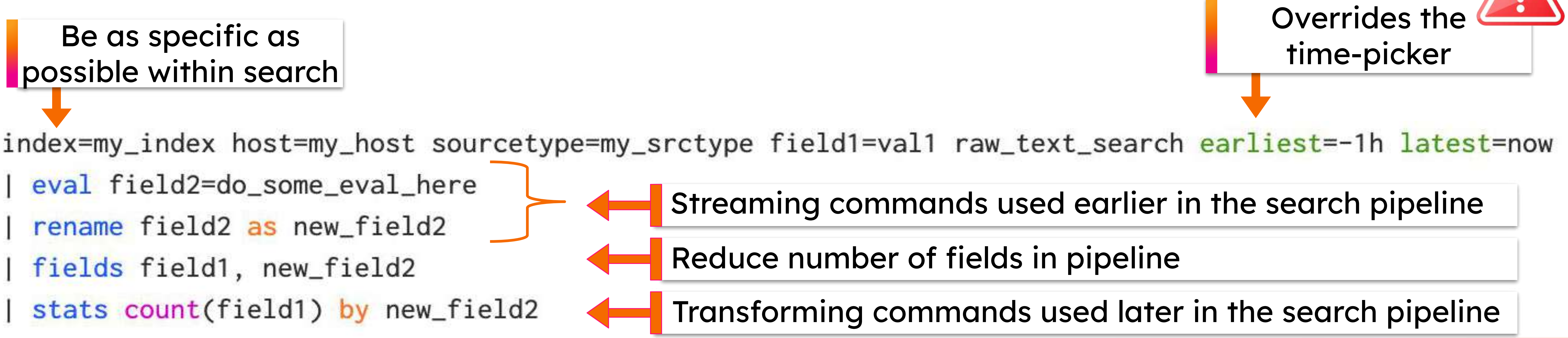
Tips for Writing Better Searches

Reduce the amount of data Splunk must Search

- Specify and limit the index(es) and other meta-fields like host(s), source(s) and sourcetype(s)
- Limit the time range for searching
- Fine-tune your searches to your unique events as much as possible
- Reduce the number of fields being passed down the SPL pipeline for processing (use fields command)

Distributed Search

- Place streaming commands earlier in the pipeline



Be as specific as possible within search

Overrides the time-picker

```
index=my_index host=my_host sourcetype=my_srctype field1=val1 raw_text_search earliest=-1h latest=now
| eval field2=do_some_eval_here
| rename field2 as new_field2
| fields field1, new_field2
| stats count(field1) by new_field2
```

Streaming commands used earlier in the search pipeline

Reduce number of fields in pipeline

Transforming commands used later in the search pipeline

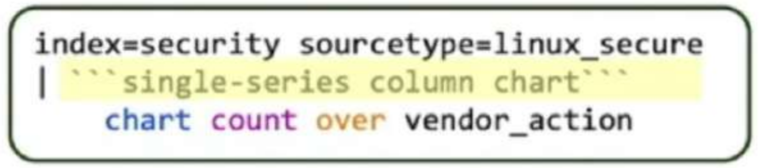
Tips for Writing Better Searches (cont.)

- **Keywords:** Search for a single word or group of words
  - e.g., error
  - e.g., error password
- **Booleans:** NOT, OR, AND
  - AND is implied
  - MUST be uppercase
  - Can use ()’s to force precedence
  - e.g., sourcetype=vendor_sales OR (sourcetype=access_combined action=purchase)
- **Phrases:** "web error"
  - Different than web AND error
- **Field Searches:** status=404, user=admin
- **Wildcard(*):** status=40* matches 40, 40a, 404, etc.
  - Starting keywords with a wildcard is very inefficient
- **Comparisons:** =,!=,<=,>=,<,>
  - e.g., status>399, user!=admin

Want to know more? Check out:
https://docs.splunk.com/Documentation/Splunk/latest/Search/Quicktipsforoptimization

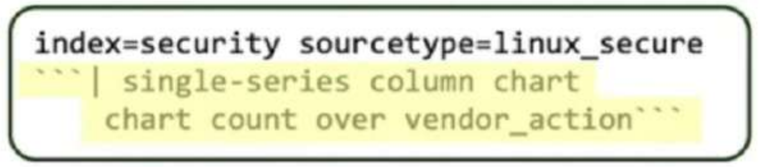
SPL Commenting

- Use three backticks (```) before and after your comment



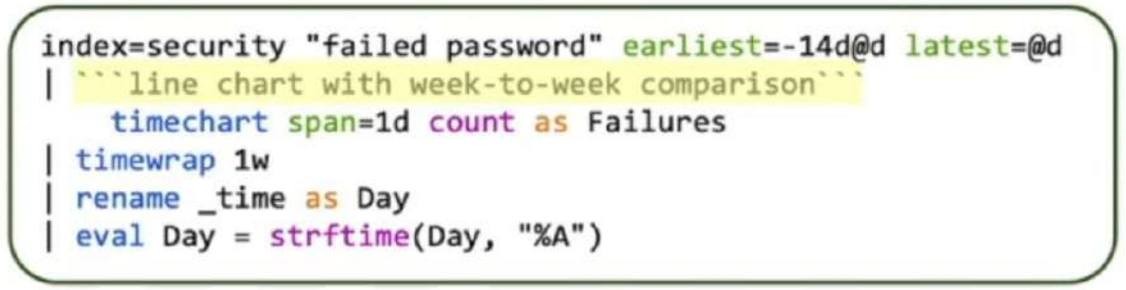
```
index=security sourcetype=linux_secure
| ```single-series column chart```
  chart count over vendor_action
```

- Comment out portions of your search to help identify and isolate problems



~~~
index=security sourcetype=linux_secure
```| single-series column chart
  chart count over vendor_action```
~~~

- To make very long SPL easier to read, add comments directly after the pipe (|)

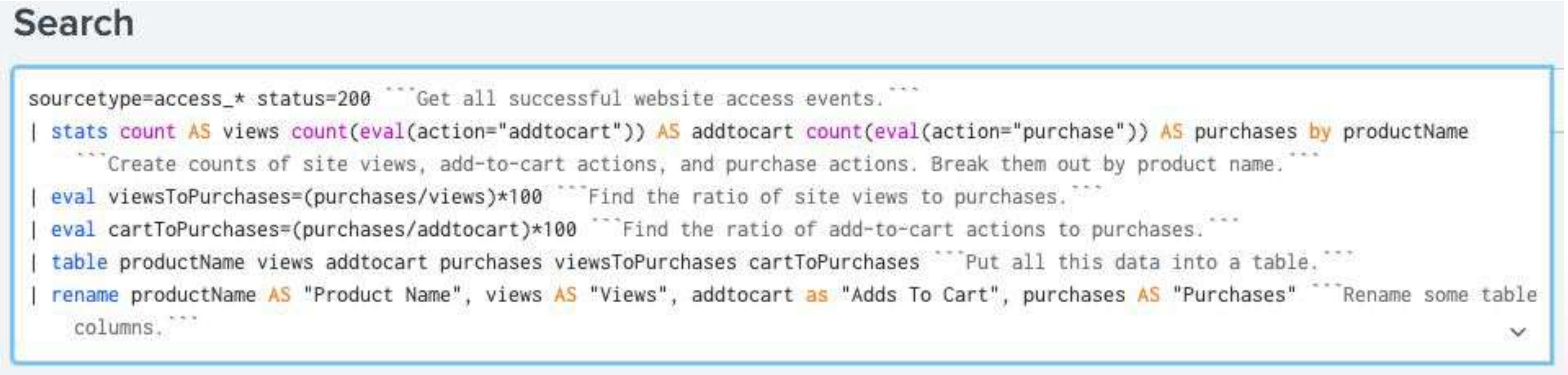


```
index=security "failed password" earliest=-14d@d latest=@d
| ```line chart with week-to-week comparison```
  timechart span=1d count as Failures
| timewrap 1w
| rename _time as Day
| eval Day = strftime(Day, "%A")
```

Useful to:

- ➢ Explain each "**step**" of a complicated search that is shared with other users
- ➢ Discuss ways of improving a search with other users
- ➢ Leave notes for yourself in unshared searches that are works in progress
- ➢ Troubleshoot searches by running them with chunks of SPL "**commented out**"

Example:



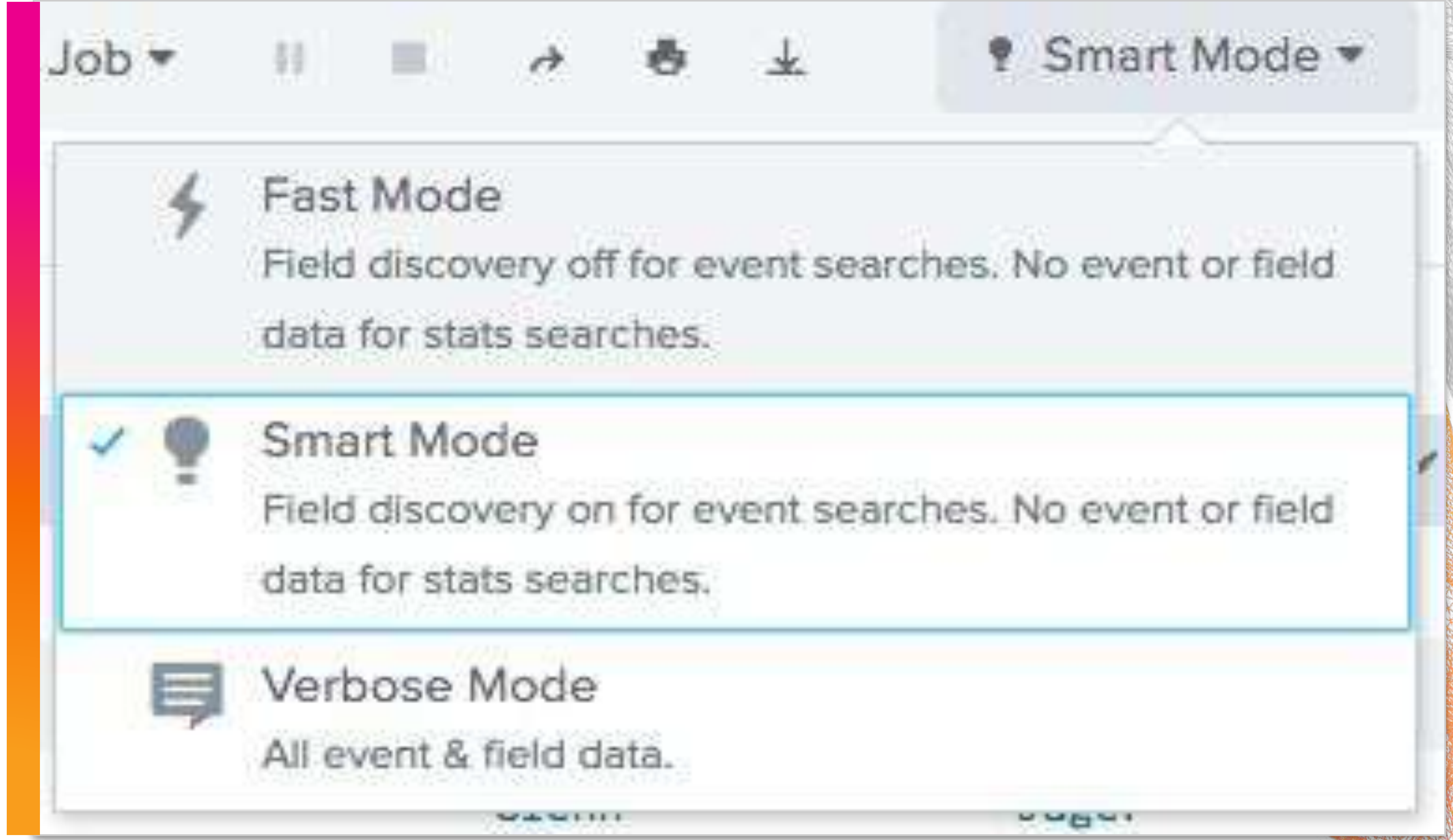
Search

~~~
sourcetype=access_* status=200 ```Get all successful website access events.```
| stats count AS views count(eval(action="addtocart")) AS addtocart count(eval(action="purchase")) AS purchases by productName
  ```Create counts of site views, add-to-cart actions, and purchase actions. Break them out by product name.```
| eval viewsToPurchases=(purchases/views)*100 ```Find the ratio of site views to purchases.```
| eval cartToPurchases=(purchases/addtocart)*100 ```Find the ratio of add-to-cart actions to purchases.```
| table productName views addtocart purchases viewsToPurchases cartToPurchases ```Put all this data into a table.```
| rename productName AS "Product Name", views AS "Views", addtocart as "Adds To Cart", purchases AS "Purchases" ```Rename some table
  columns.```
~~~

Want to know more? Check out: https://docs.splunk.com/Documentation/Splunk/latest/Search/Comments

Splunk Search Modes

- **Fast:** emphasizes speed over completeness
- **Smart:** balances speed and completeness (default)
- **Verbose:** emphasizes completeness



Fast Mode
Field discovery off for event searches. No event or field data for stats searches.

✓ Smart Mode
Field discovery on for event searches. No event or field data for stats searches.

Verbose Mode
All event & field data.

Want to know more? Check out: https://docs.splunk.com/Documentation/Splunk/latest/Search/Changethesearchmode

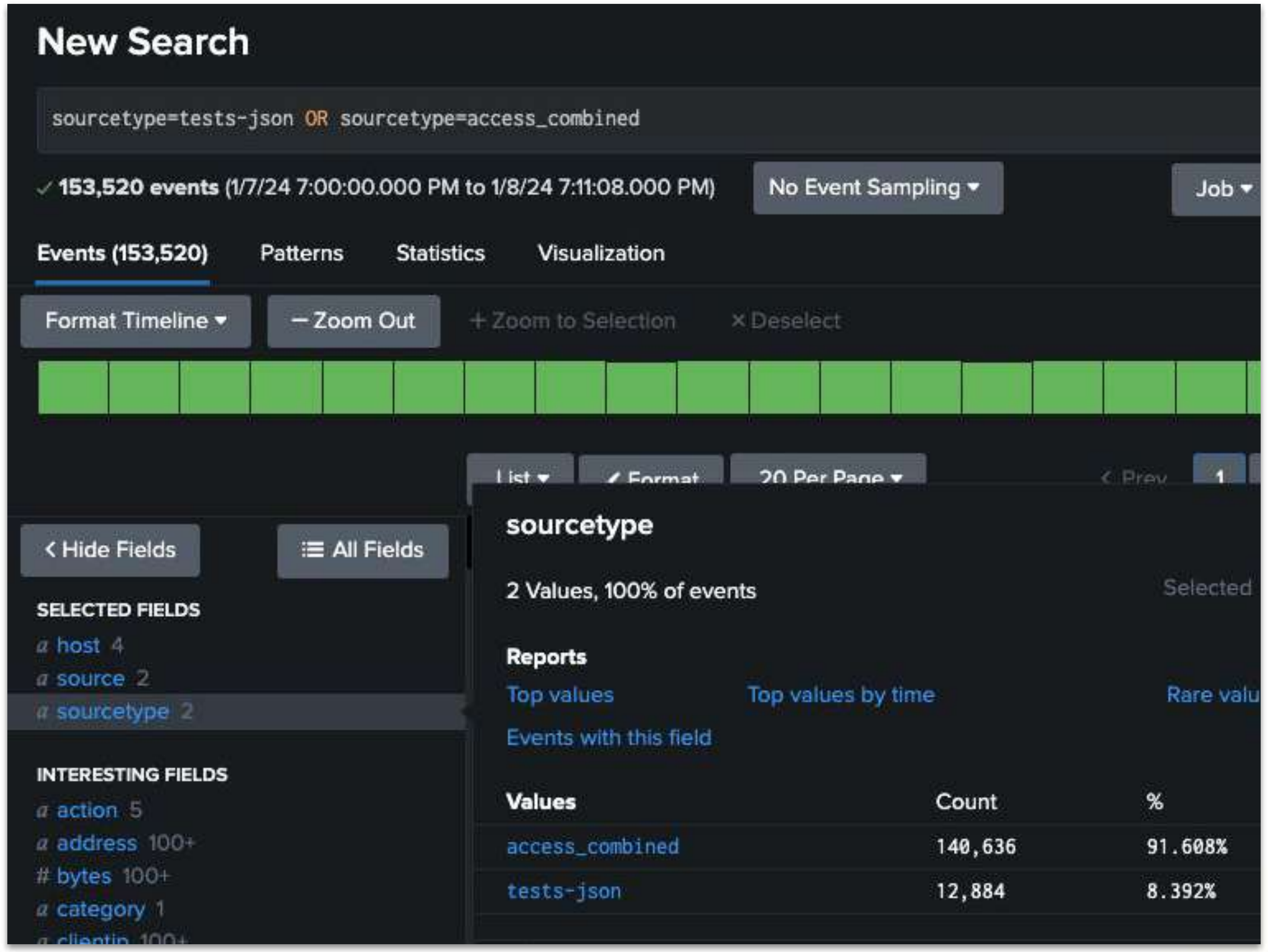
Popular SPL Commands

LAB EXERCISE 1 5 MINS

Searching w/ Keywords, Field-Value Pairs & Booleans

Tasks

1. Search combined app log + web log data
2. Search app log data for host “test-01” AND platform “iOS”
3. Search app log data for host “test-01” AND NOT platform “iOS”
4. **Hints:**
   - App log data sourcetype: `tests-json`
   - Web log data sourcetype: `access_combined`



New Search

```
sourcetype=tests-json OR sourcetype=access_combined
```

✓ **153,520 events** (1/7/24 7:00:00.000 PM to 1/8/24 7:11:08.000 PM)

Events (153,520) Patterns Statistics Visualization

SELECTED FIELDS
- a host 4
- a source 2
- a sourcetype 2

INTERESTING FIELDS
- a action 5
- a address 100+
- # bytes 100+
- a category 1

sourcetype

2 Values, 100% of events

Reports

Top values Top values by time Rare valu

Events with this field

Values	Count	%
access_combined	140,636	91.608%
tests-json	12,884	8.392%

Outcomes & value:

- Detect and resolve issues by narrowing in on exact events (needles in haystacks)

LAB EXERCISE 2 3 MINS

The stats Command

Use the stats command to turn data into aggregate tables!

Calculates statistics based on fields in your events!

Stats functions:

- c / count / sum / distinct_count / dc
- min / max
- avg / stdev
- median / perc90 perc<int1-100>
- list / values
- earliest / latest

Syntax:

```
<your search> | stats <function> <by clause>
```

Exercise #2: Track number of errors vs. successes as well as average load times and group the results by platform

- Hints:
  - Focus on app log events
  - You can use combinations of more than one function from list above
  - Sort results in descending order (based on count value)

Outcomes & value:

- Group data to find patterns to detect future problems, report on current situation & context

LAB EXERCISE 3 3 MINS

The `timechart` Command

Use the `timechart` command to turn data into timecharts!

Timechart functions:

- `count` / `sum`
- `min` / `max`
- `avg` / `stdev`
- `median` / `perc90`
- `earliest` / `latest`
- `distinct_count` / `dc` / `estdc`

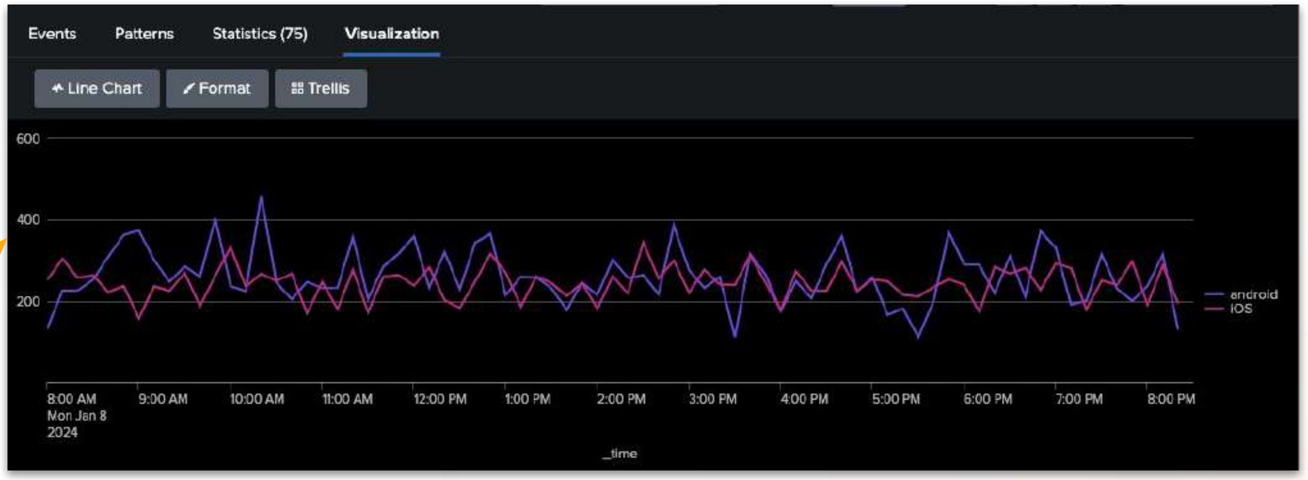
Creates a time series chart with a corresponding table of statistics

Syntax:

```
<your search> | timechart <function> <by clause>
```

Exercise #3: Chart median load times across platforms over time

- Hints:
  - Focus on app log events
  - You only need to use 1 function from the list above
  - Visualize the results in a "Line Chart"
    - Edit formatting options to match style in screenshot



Outcomes & value:

- Report and analyze patterns and trends, communicate anomalies to management

LAB EXERCISE 4 5-10 MINS

The `eval & where` Commands

Use `eval` command to calculate expressions and create new fields
Use `where` function to filter based on Boolean logic

Eval/where `functions`:

- +, -, *, /
- 'fieldnames' / "strings"
- `if` / `case` / `coalesce`
- `isnull` / `isnotnull`

Syntax:

```
<your search>
| eval <field>=<expression>
| where <eval-expression>
```

Example:

```
<your search>
| eval msg=if(status==200, “OK”, “Error”)
| where msg=”Error”
```

Exercise #4: Find apps with high errors **or** load times

- Hints:
  - Focus on app log events
  - Use stats + combinations of count, eval, and avg functions
    - Use eval within stats command once, and once as its own command
  - High errors or load times = If the number of errors x the avg load time is more than 10K
  - Sort results in descending order based on newly created field (from eval command)
  - Use where clause at the end to filter events where the newly created field > 10,000

Outcomes & value:

- Improve collaboration and detections with common field aliases and new combinations of fields

Other Popular SPL Commands

Rename fields with rename:

- `sourcetype=tests-json | rename error as Error_Description`

Deduplicate repeated events with dedup:

- `sourcetype=tests-json | dedup ip`

Show only key fields in events or table view with fields/table:

- `sourcetype=tests-json | fields _time platform type error`
- `sourcetype=tests-json | table _time platform type error`

Get most recent/oldest or least/most common events with head/tail/rare/top:

- `sourcetype=tests-json | head 10`
- `sourcetype=tests-json | top 3 platform type`

Outcomes & value:

- Detect and report on important information in your data

Plus 100+ others:
https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/ListOfSearchCommands

Common Use Cases from Real Customers

ITOps, Olly, SecOps, Biz Analytics, & IoT

splunk>

Splunk Use Cases & Customer Examples

IT Operations

Predict service-level degradation before it occurs

Application Observability

Improve app performance and reliability using app logs and infrastructure

Security & Compliance

Speed up security investigations and reduce the impact of insider threats

Business Analytics

Drive more orders with marketing campaigns across website and mobile

Internet of Things

Monitor and resolve problems from 10,000s of sensors in real time

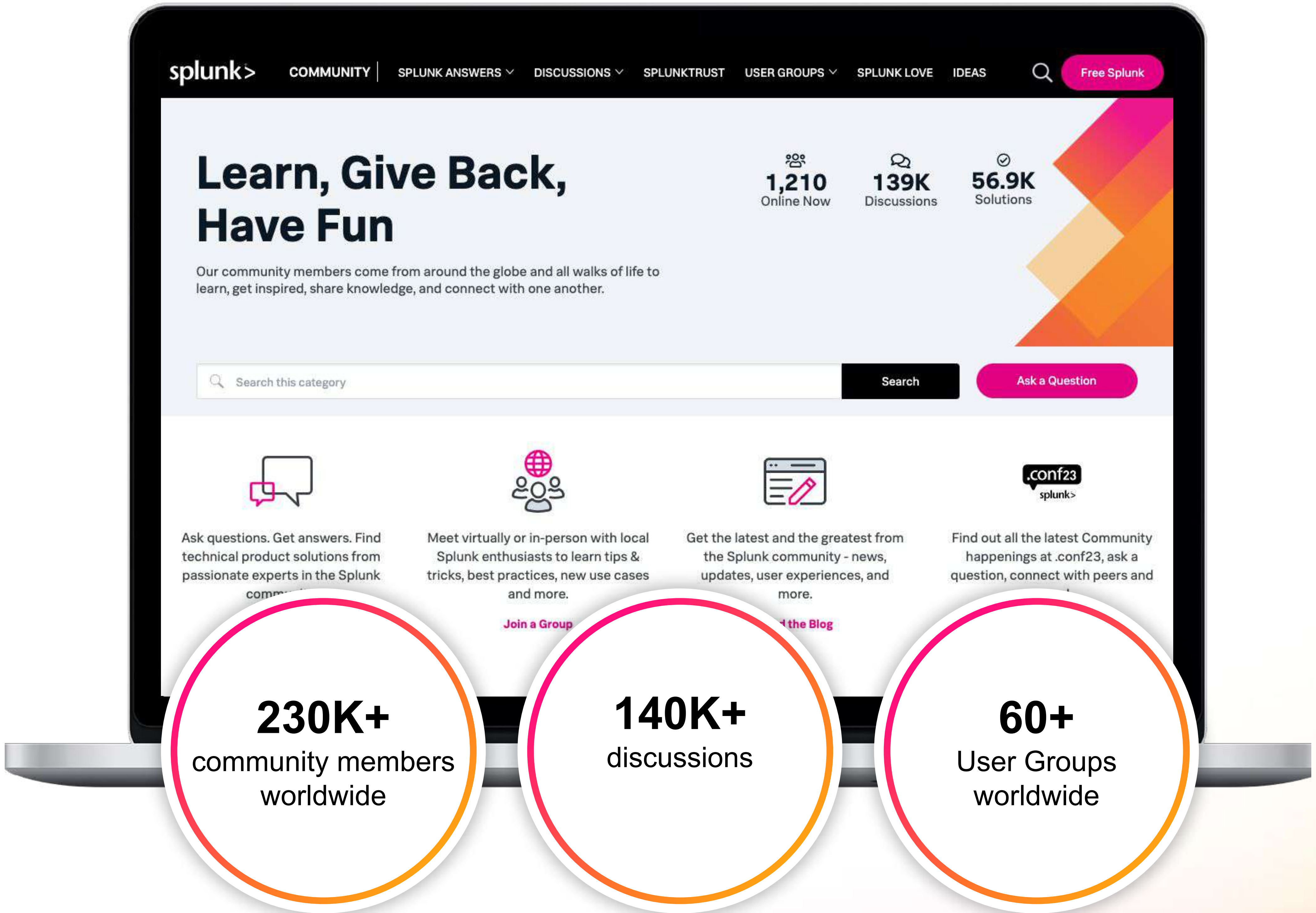
Resources

Where to go from here?

Splunk Community

https://community.splunk.com

- A free way to connect, learn, have fun, and find success with Splunk
- Ask questions, get answers, and find solutions from passionate experts in the community
- Meet in-person or virtually with like-minded enthusiasts, in your area or by interest
- Search for, vote on, or submit your own ideas for new enhancements for any product or solution



Learn, Give Back, Have Fun

1,210 Online Now

139K Discussions

56.9K Solutions

Our community members come from around the globe and all walks of life to learn, get inspired, share knowledge, and connect with one another.

Ask questions. Get answers. Find technical product solutions from passionate experts in the Splunk comm

Meet virtually or in-person with local Splunk enthusiasts to learn tips & tricks, best practices, new use cases and more.

Join a Group

Get the latest and the greatest from the Splunk community - news, updates, user experiences, and more.

the Blog

Find out all the latest Community happenings at .conf23, ask a question, connect with peers and

230K+ community members worldwide

140K+ discussions

60+ User Groups worldwide

Splunk Events

https://splunk.com/events

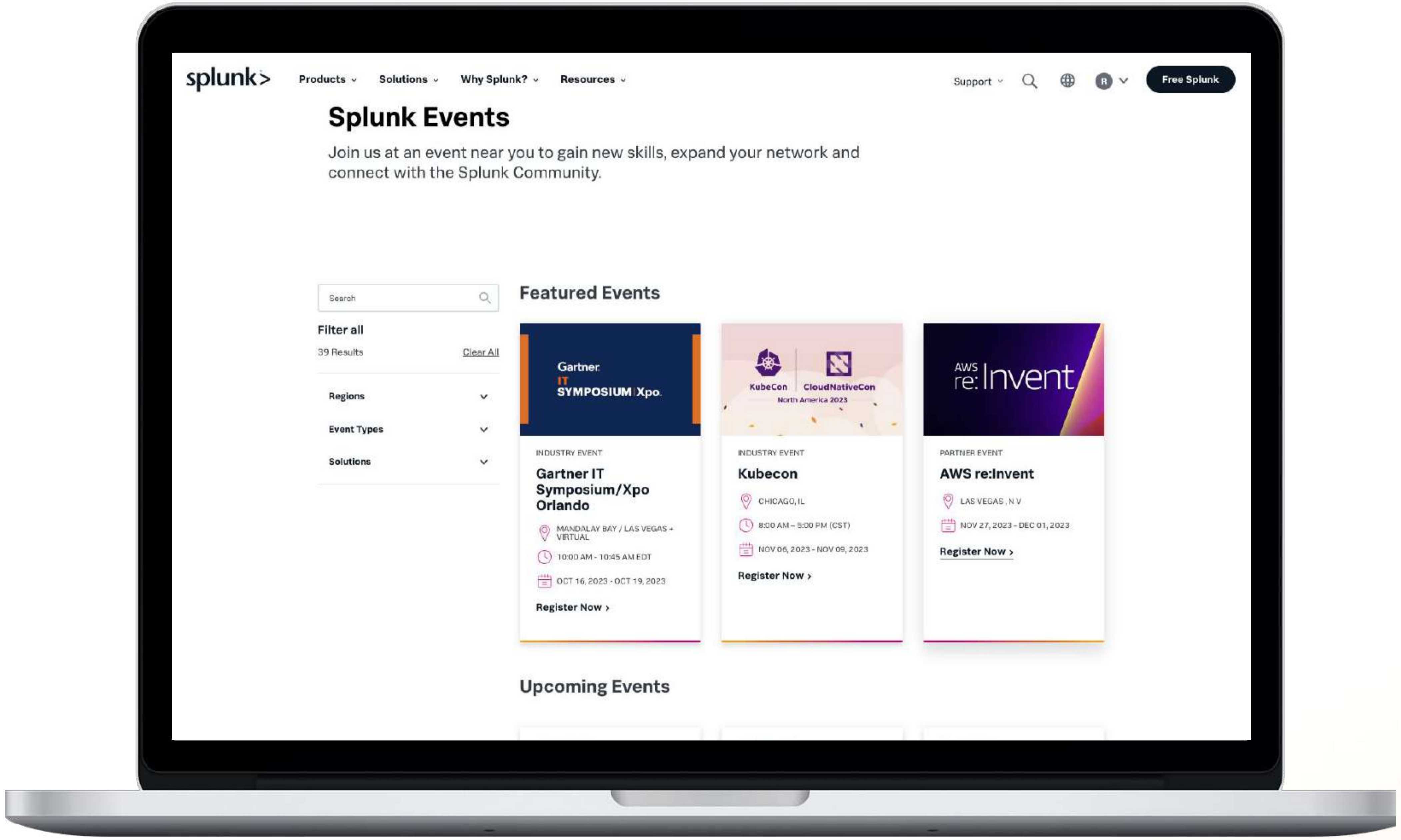
- Expand your network and connect with the global and local Splunk community

.conf

https://conf.splunk.com

- Join us at .conf next summer!

- Hundreds of on-demand sessions from product updates to learning new Splunk skills!



Splunk Events

Join us at an event near you to gain new skills, expand your network and connect with the Splunk Community.

Filter all

39 Results Clear All

Featured Events

INDUSTRY EVENT

Gartner IT Symposium/Xpo Orlando

MANDALAY BAY / LAS VEGAS + VIRTUAL

10:00 AM - 10:45 AM EDT

OCT 16, 2023 - OCT 19, 2023

Register Now ›

INDUSTRY EVENT

Kubecon

CHICAGO, IL

8:00 AM – 5:00 PM (CST)

NOV 06, 2023 - NOV 09, 2023

Register Now ›

PARTNER EVENT

AWS re:Invent

LAS VEGAS , N V

NOV 27, 2023 - DEC 01, 2023

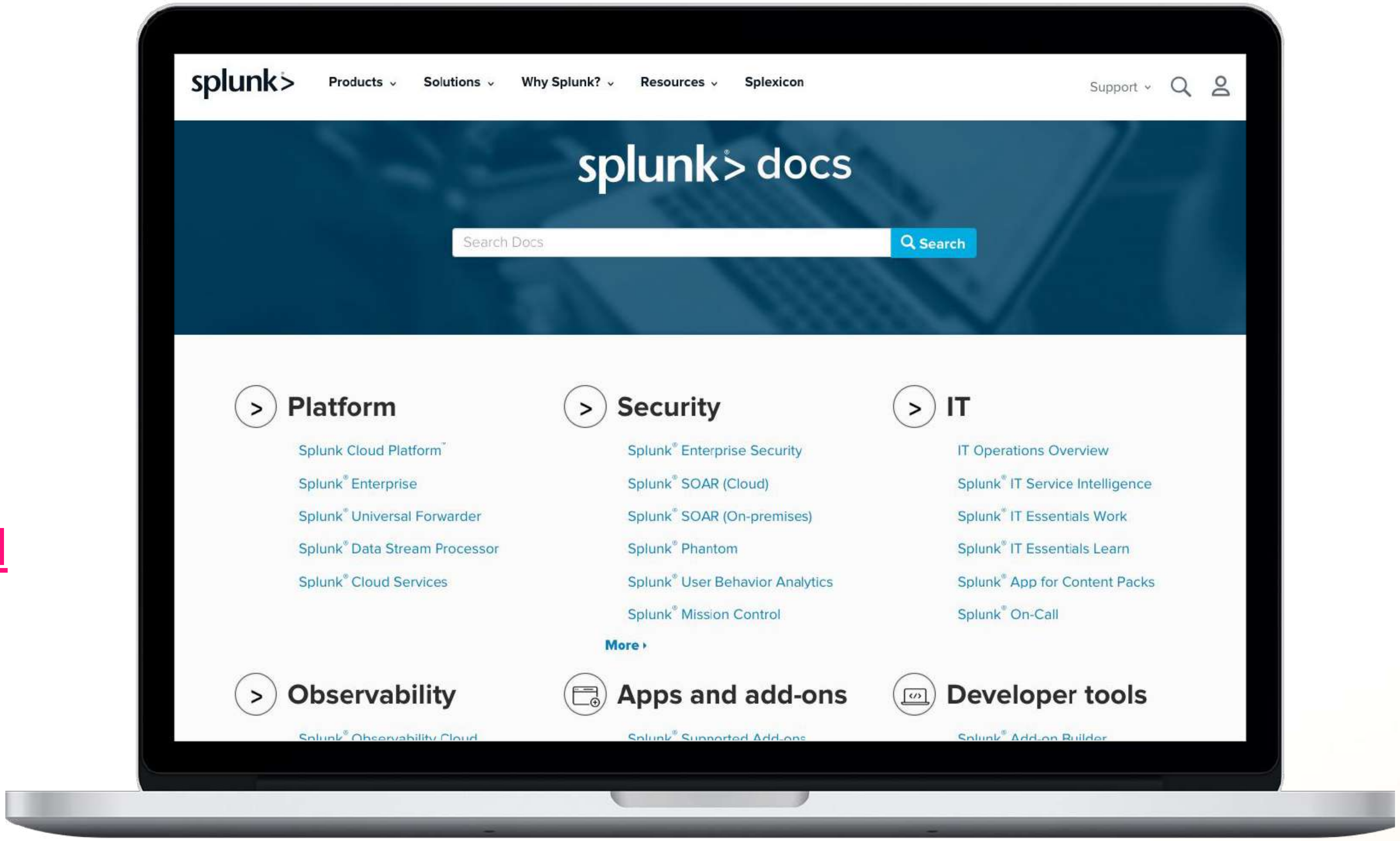
Register Now ›

Upcoming Events

Documentation

https://docs.splunk.com

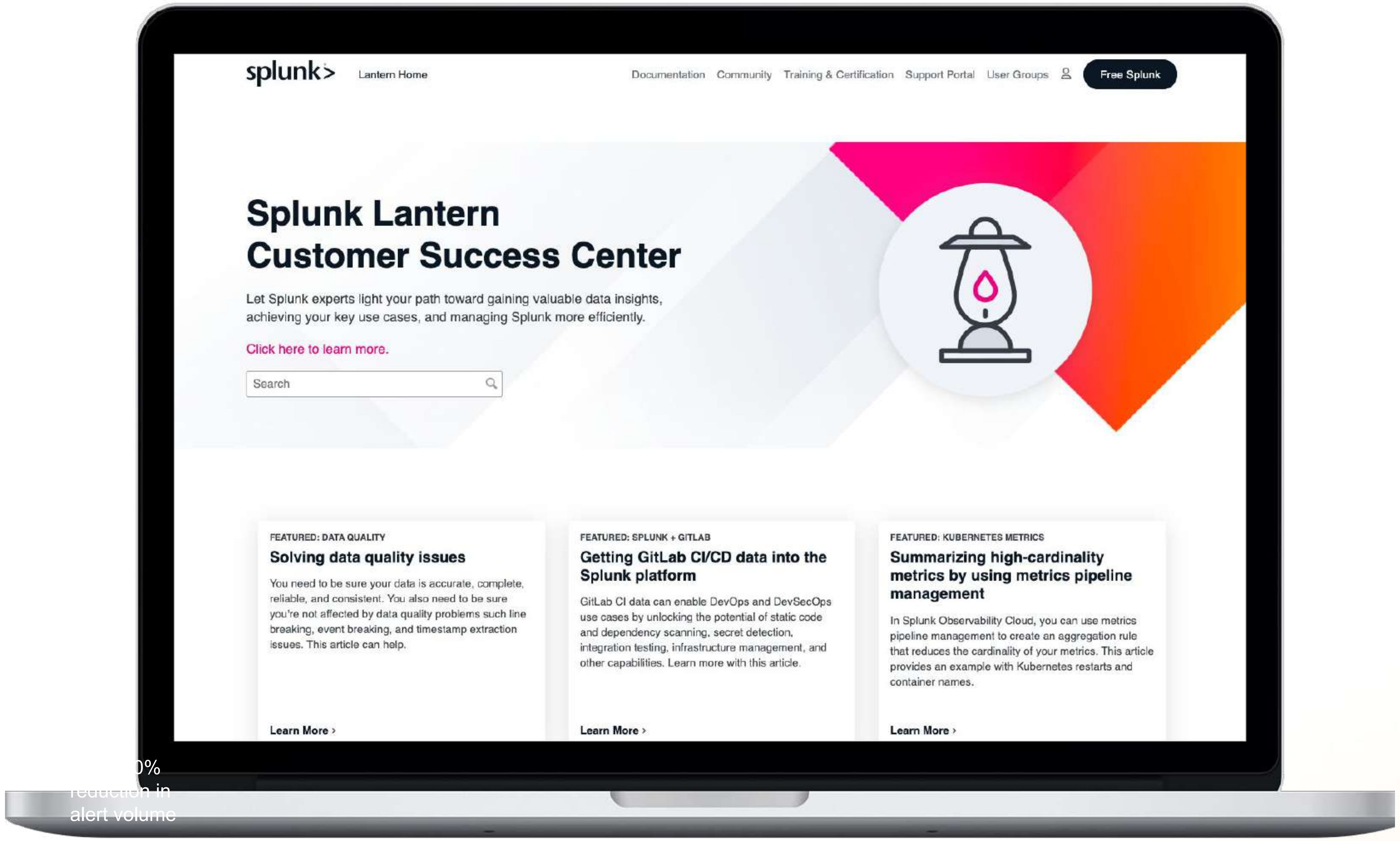
- Search reference for SPL
- Step-by-step tutorials
  Search:
  https://splk.it/SplunkSearchTutorial
  Dashboard Studio:
  https://splk.it/SplunkDashStudioTutorial
- Product references
- Procedures/guides
- And more!



Splunk Lantern

https://lantern.splunk.com

- Use case library
- Step-by-step procedures
- Map use cases to data sources
- Splunk Success Framework to realize value across your organisation



Splunk Lantern
Customer Success Center

Let Splunk experts light your path toward gaining valuable data insights, achieving your key use cases, and managing Splunk more efficiently.

Click here to learn more.

FEATURED: DATA QUALITY

Solving data quality issues

You need to be sure your data is accurate, complete, reliable, and consistent. You also need to be sure you're not affected by data quality problems such line breaking, event breaking, and timestamp extraction issues. This article can help.

Learn More ›

FEATURED: SPLUNK + GITLAB

Getting GitLab CI/CD data into the Splunk platform

GitLab CI data can enable DevOps and DevSecOps use cases by unlocking the potential of static code and dependency scanning, secret detection, integration testing, infrastructure management, and other capabilities. Learn more with this article.

Learn More ›

FEATURED: KUBERNETES METRICS

Summarizing high-cardinality metrics by using metrics pipeline management

In Splunk Observability Cloud, you can use metrics pipeline management to create an aggregation rule that reduces the cardinality of your metrics. This article provides an example with Kubernetes restarts and container names.

Learn More ›

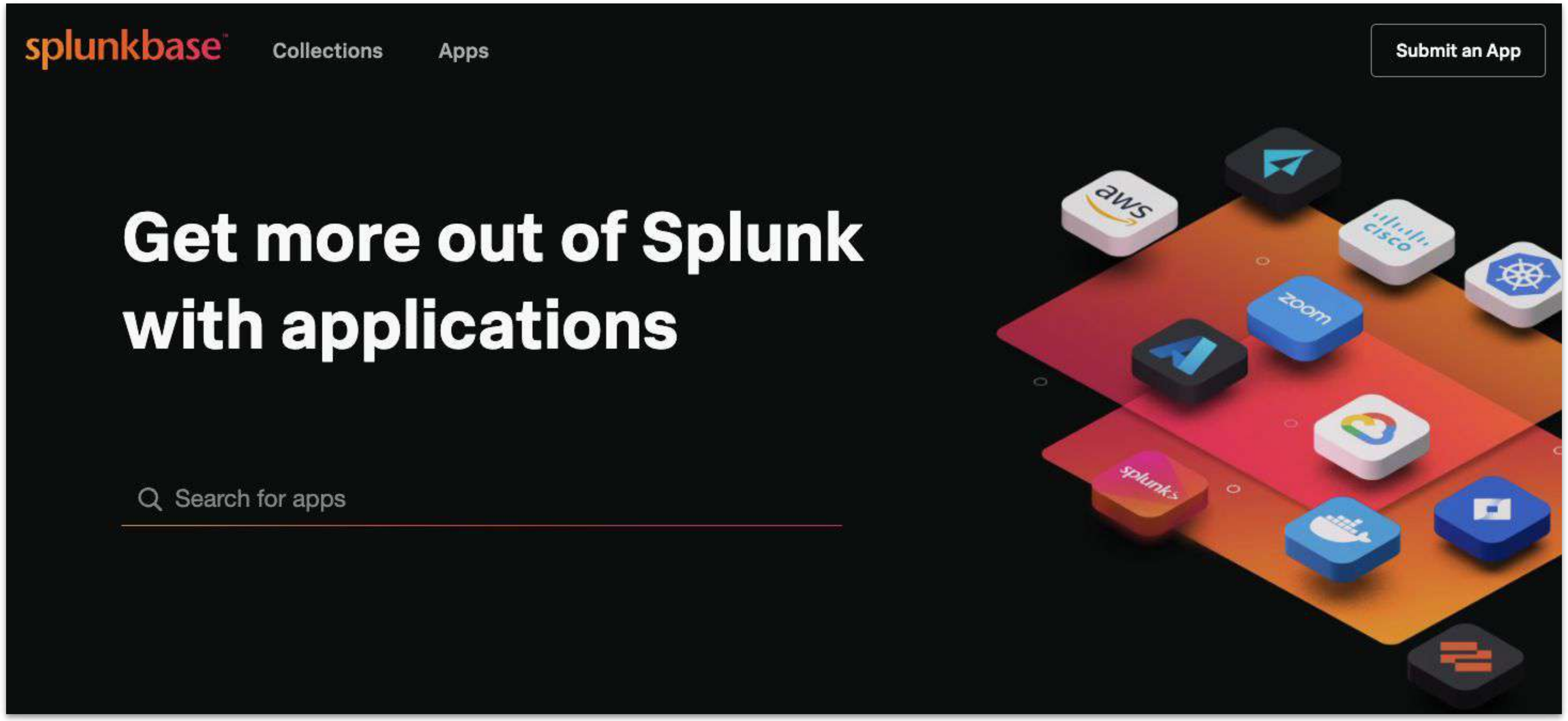
0%
reduction in
alert volume

Splunkbase

Splunkbase has 3100+ apps

Enable new use cases and extend your teams' Splunk capabilities:

https://splunkbase.splunk.com



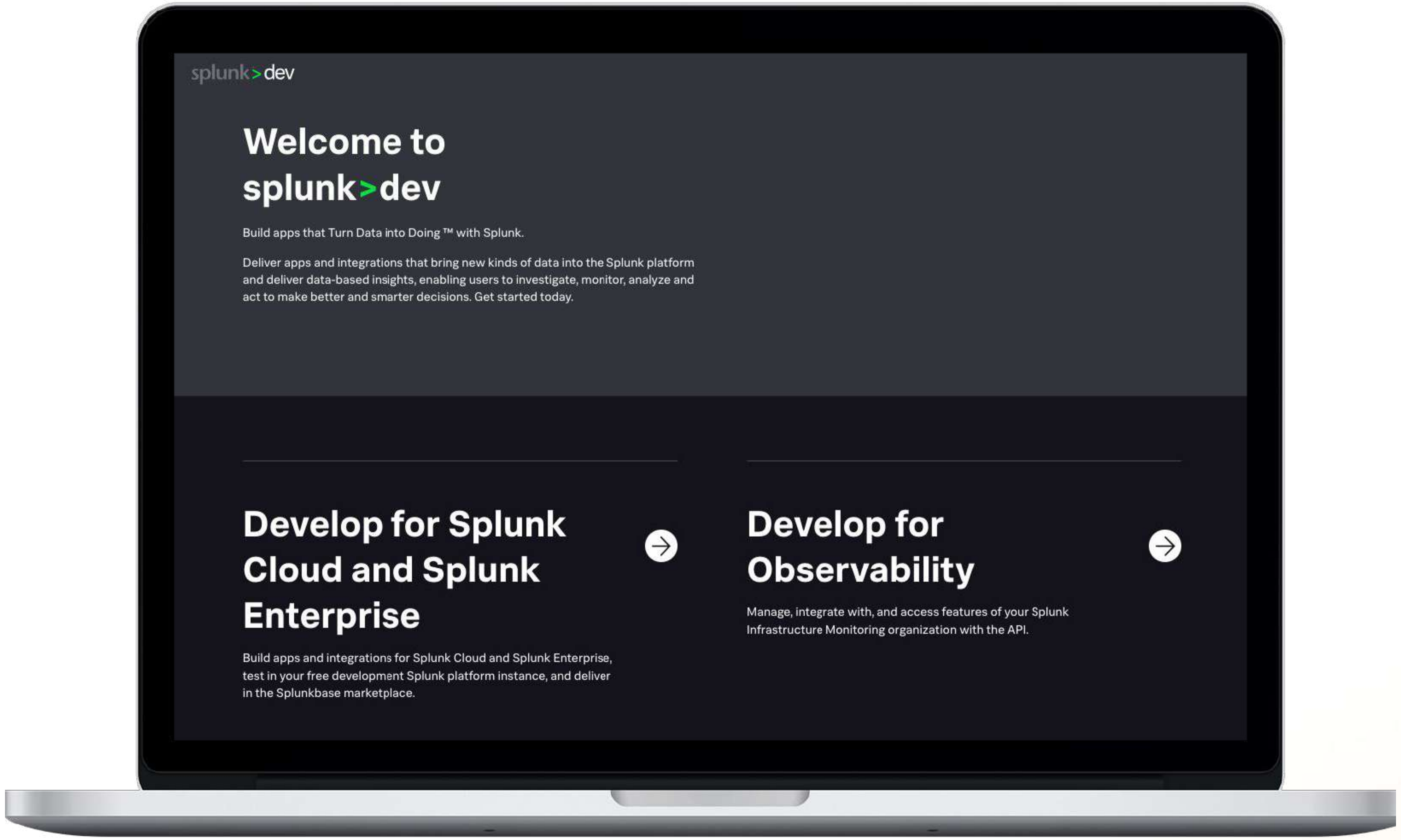
Get more out of Splunk with applications

- 2100+ apps and add-ons
- Pre-built searches, reports, visualisations and integrations for specific use cases and technologies
  - Use cases include:
    - IT Ops, Security, Observability, Business Analytics, IoT & Industrial Data
    - Financial Services, Retail, Telecom, Healthcare, Energy
- Download apps and customize them based on your requirements
- Fast time to value from your data
- Build and contribute your own apps!

Developer Resources

https://dev.splunk.com

- Developer Guide
- API Reference
- Tutorials
- Downloads
  APIs, libraries, tools
- Code examples
- Free Developer licence



Welcome to splunk>dev

Build apps that Turn Data into Doing ™ with Splunk.

Deliver apps and integrations that bring new kinds of data into the Splunk platform and deliver data-based insights, enabling users to investigate, monitor, analyze and act to make better and smarter decisions. Get started today.

Develop for Splunk Cloud and Splunk Enterprise

Build apps and integrations for Splunk Cloud and Splunk Enterprise, test in your free development Splunk platform instance, and deliver in the Splunkbase marketplace.

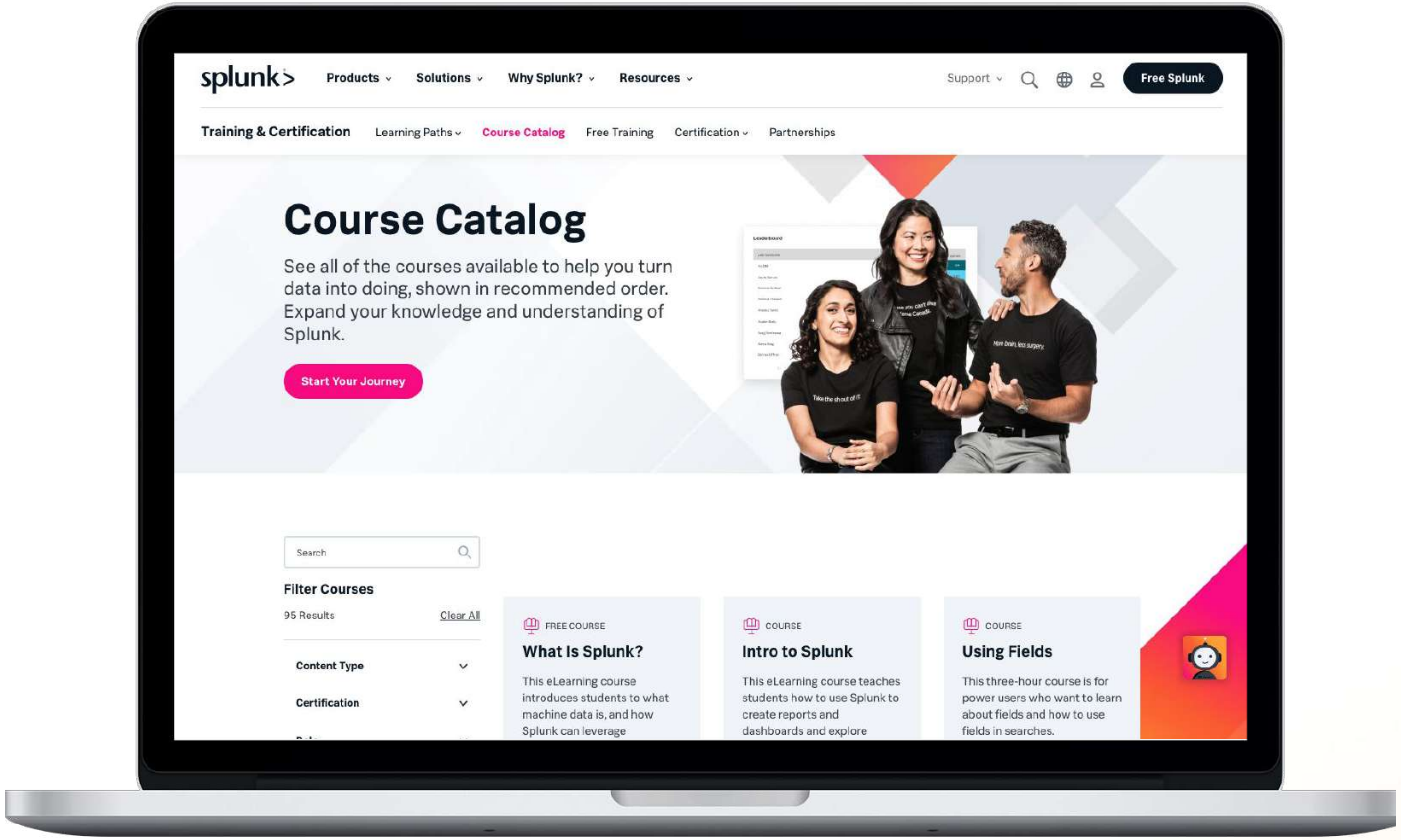
Develop for Observability

Manage, integrate with, and access features of your Splunk Infrastructure Monitoring organization with the API.

Training & Certification

https://splunk.com/training

- **Online education classes**
  Instructor-led and self-paced eLearning
- **Certification tracks for different roles**
  User, Power User, Admin, Architect and Developer
- **Splunk Education Rewards**
  Complete training and receive points that you can redeem for Splunk swag!
- **Free education!**
  Free single-subject eLearning courses to kick start your Splunk learning



Course Catalog

See all of the courses available to help you turn data into doing, shown in recommended order. Expand your knowledge and understanding of Splunk.

Filter Courses

95 Results

FREE COURSE
What Is Splunk?
This eLearning course introduces students to what machine data is, and how Splunk can leverage

COURSE
Intro to Splunk
This eLearning course teaches students how to use Splunk to create reports and dashboards and explore

COURSE
Using Fields
This three-hour course is for power users who want to learn about fields and how to use fields in searches.

Thank you!

splunk>