Using Splunk

Course Outline

- Introducing Splunk's User Interface
- Searching
- Using Fields in Searches
- Creating Reports and Visualizations
- Using Pivot
- Working with Dashboards

Introducing Splunk's User Interface

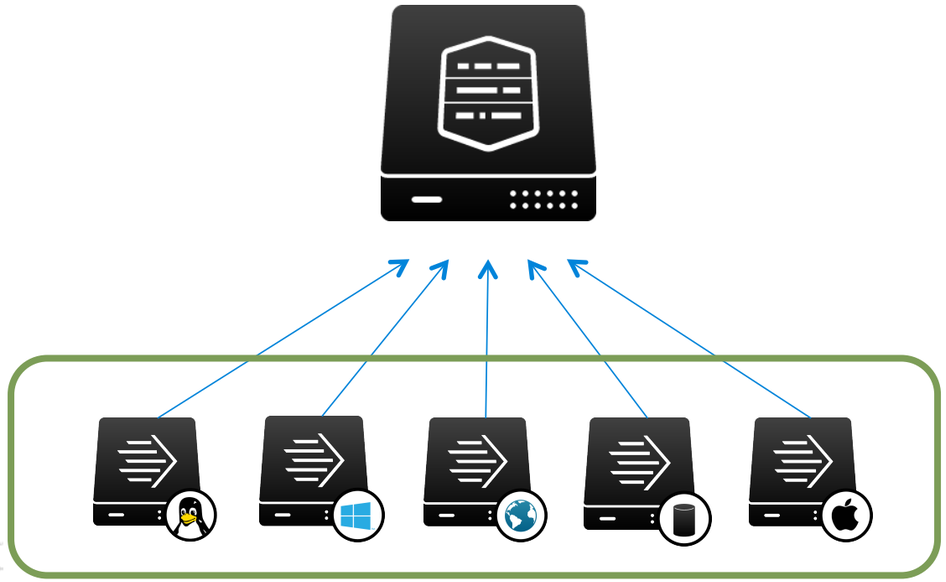
Module Objectives

- Understand the uses of Splunk
- Define Splunk apps
- Learn basic navigation in Splunk

Got Data?

- Computers
- Network devices
- Virtual machines
- Internet devices
- Communication devices
- Sensors
- Databases
- ***Any source***

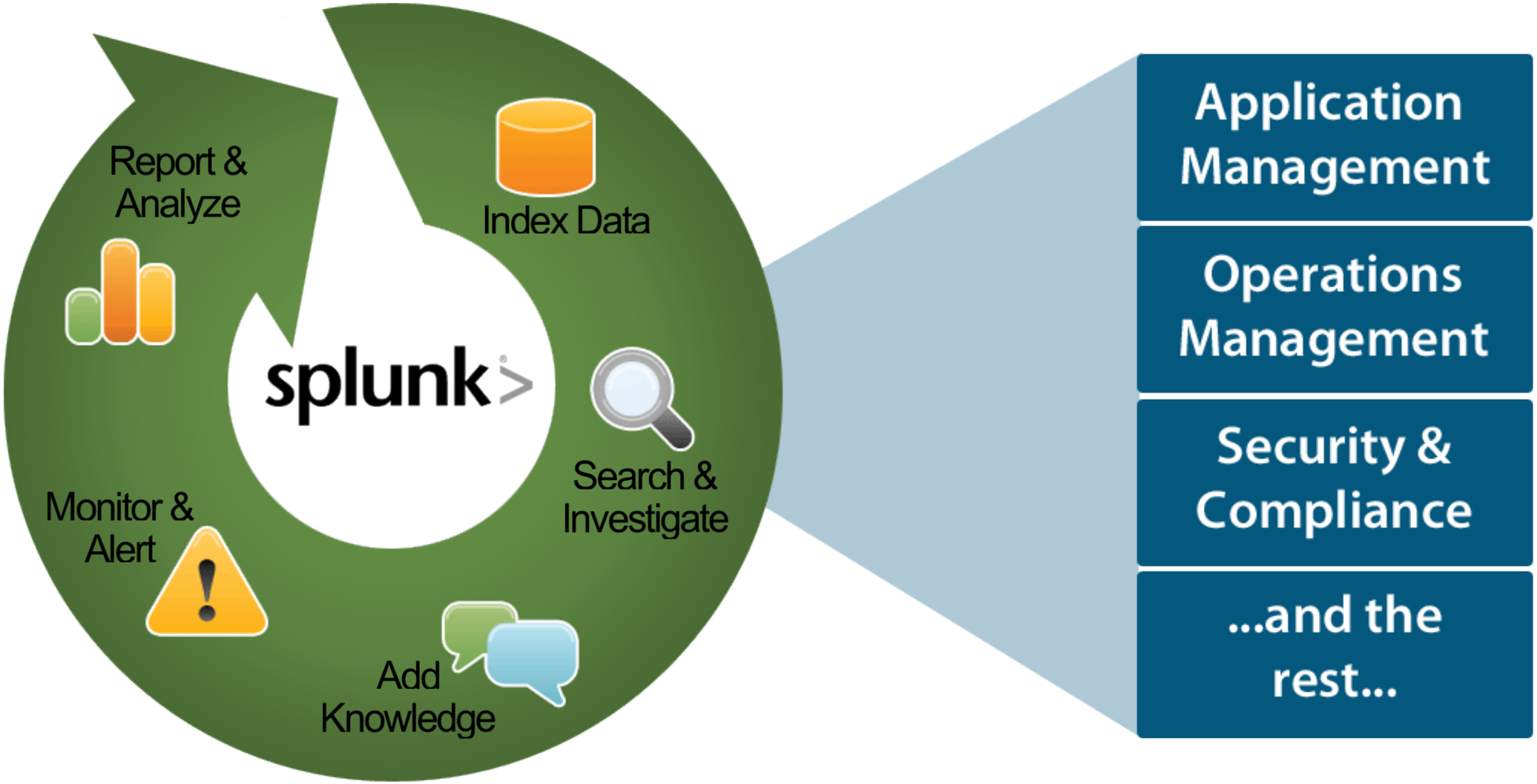
- Logs
- Configurations
- Messages
- Call detail records
- Clickstream
- Alerts
- Metrics
- Scripts
- Changes
- Tickets
- ***Any data***



Indexes any data from any source

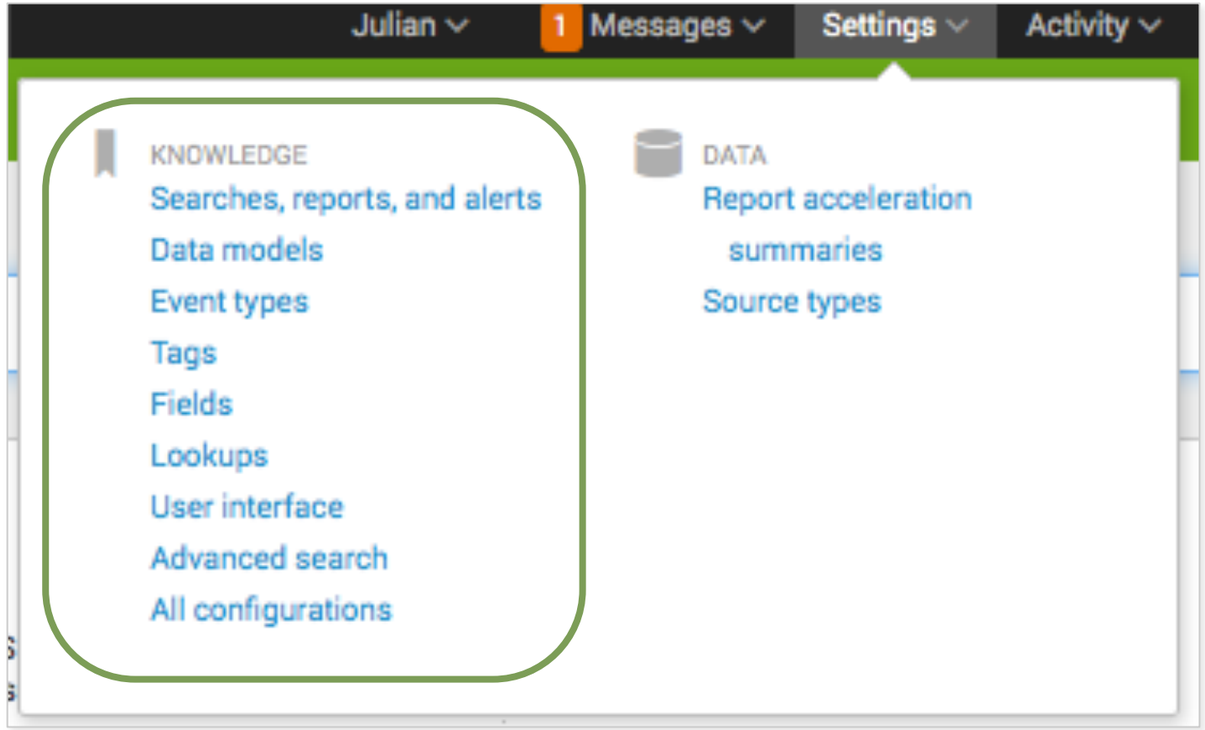
 |

One Splunk. Many Uses.



Describe Knowledge Objects

- Knowledge objects make your data more robust while providing ways to interpret, classify, enrich, and normalize (organize) your events
- Create knowledge objects to add value to your data
  - Can be reused and shared
- Click **Settings** to access your knowledge objects

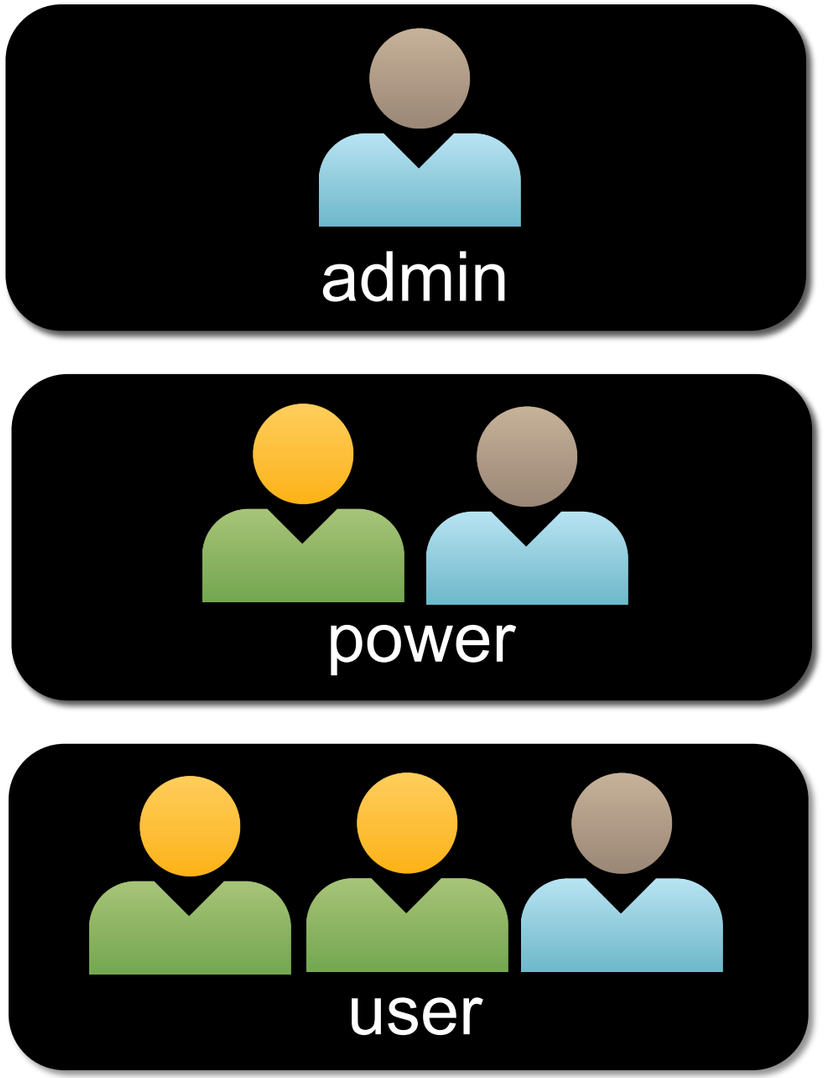


Note

http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/WhatisSplunkknowledge

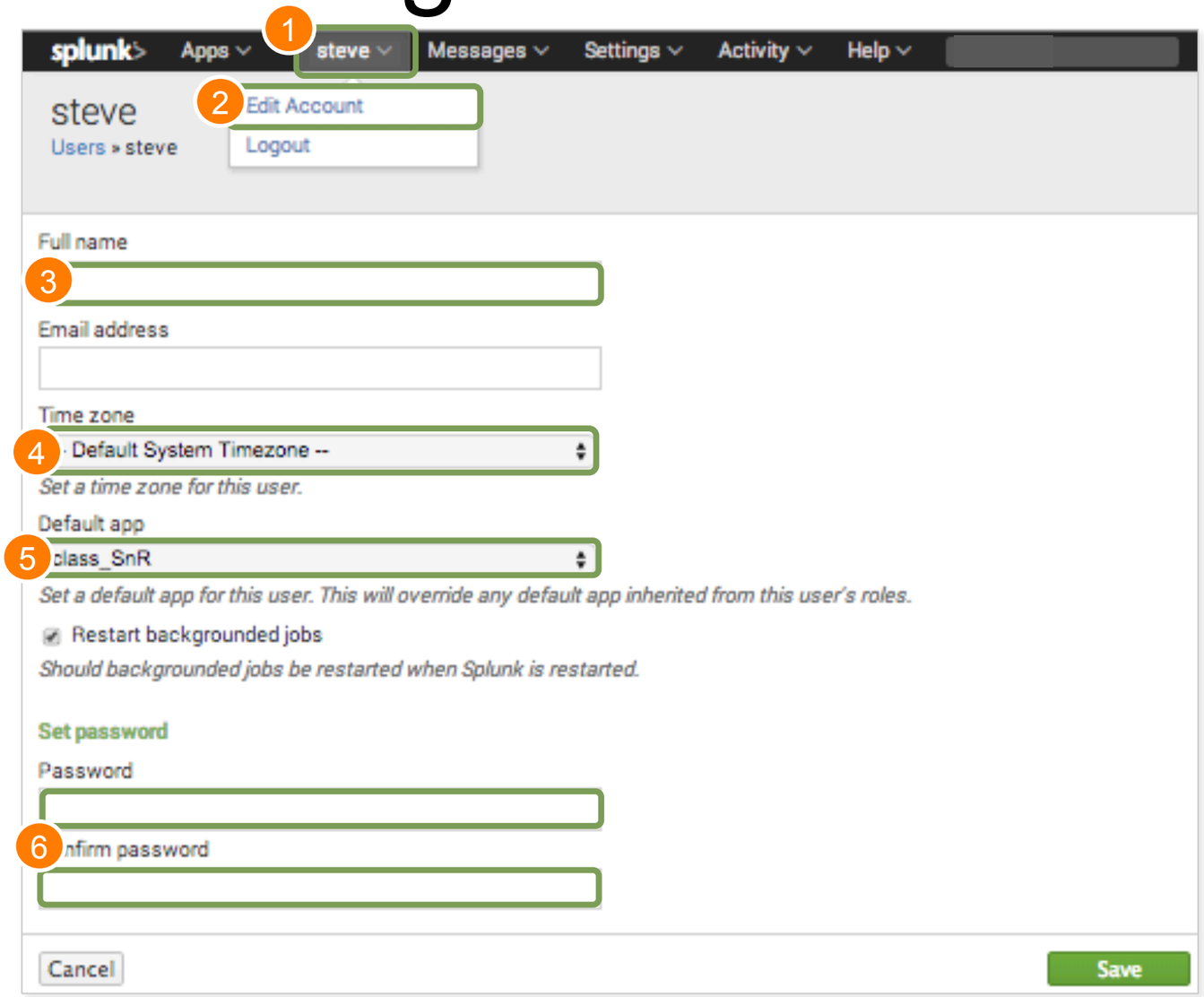
Users and Roles

- Splunk users are assigned roles
  - Roles determine capabilities and data access
- Out of the box, there are 3 main roles:
  - Admin
  - Power
  - User
- Splunk administrators can create additional roles
- This class is written for the **power user** role



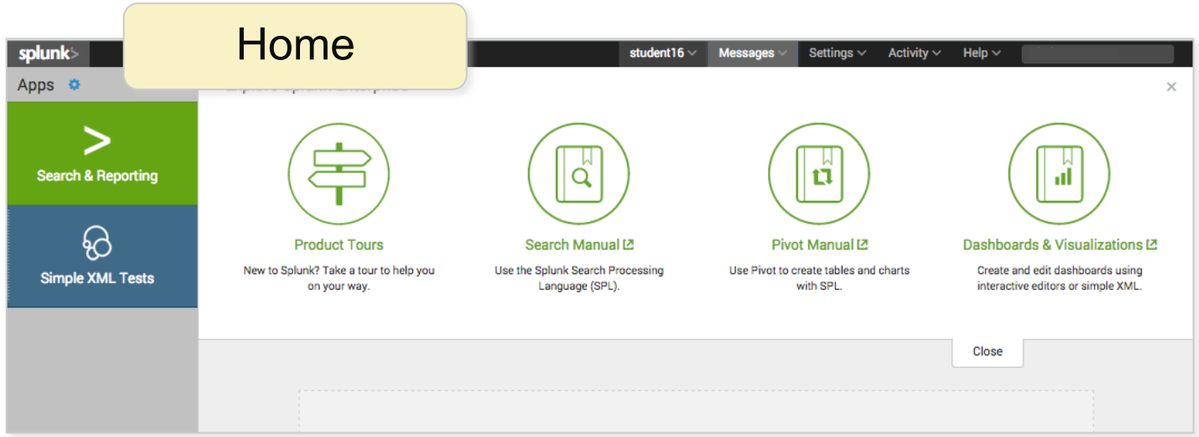
User Settings

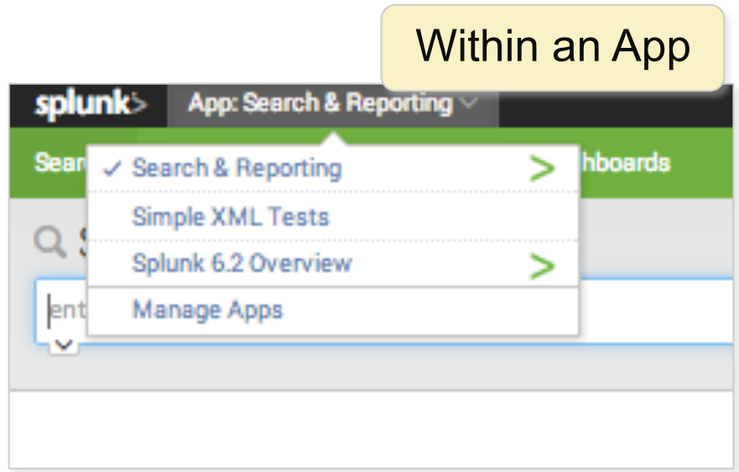
1. Click your name
2. Click Edit Account
3. Set **Full name** to the name you want to display in the main menu
4. Set **Time zone** to show and convert the time of each event in your time zone
5. Set a default app
6. If applicable, change your password



What are Apps?

- Apps allow different workspaces, tailored to a specific use case or user role, to exist on a single Splunk instance
- This class focuses on the Search & Reporting app (also called the Search app)
- Administrators can install additional apps to your Splunk instance from http://splunkbase.splunk.com



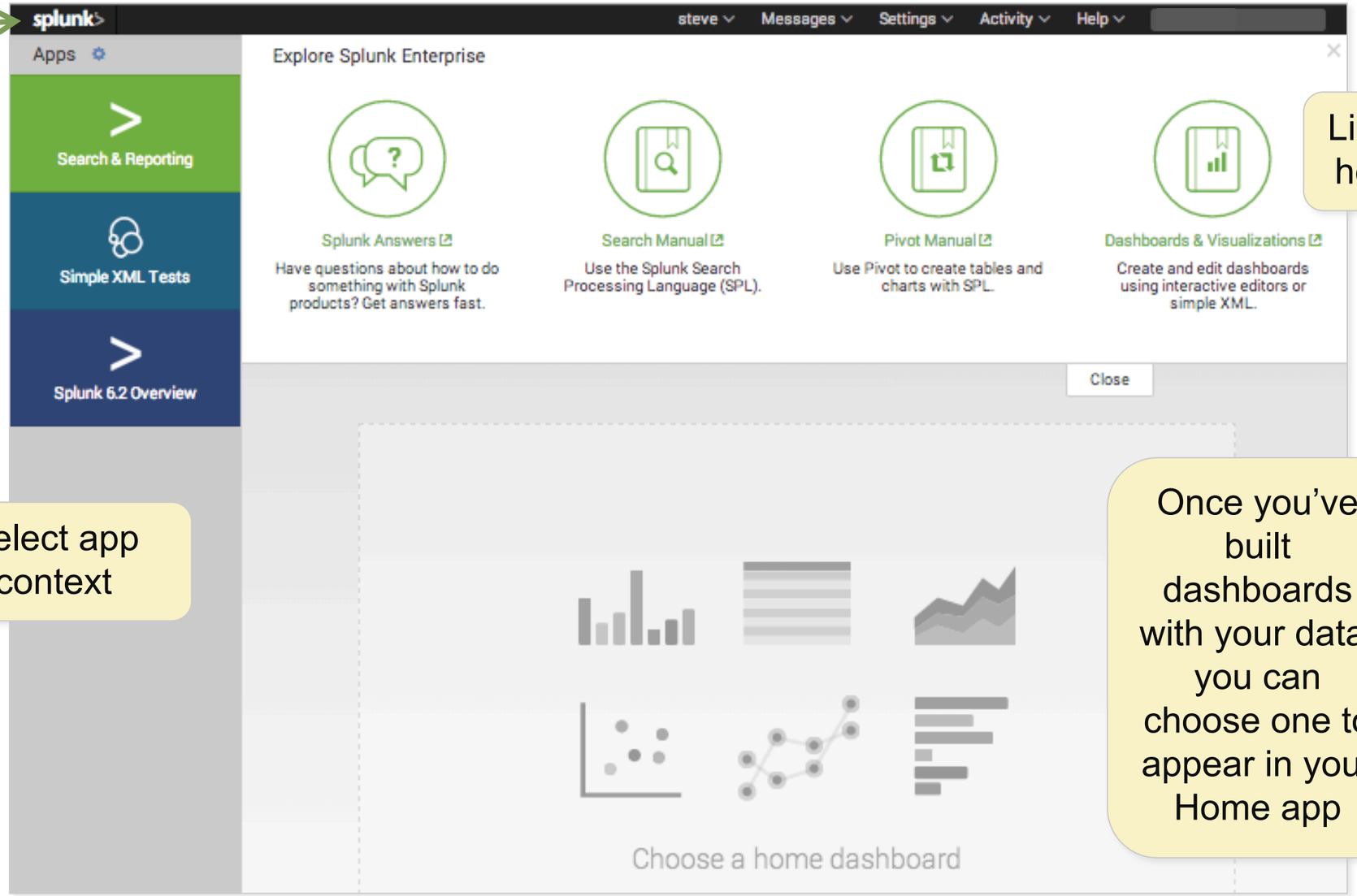


Note

Simply put, a Splunk app is a collection of files. Some apps are more robust and contain data inputs, knowledge objects, and UI elements.
http://docs.splunk.com/Documentation/Splunk/latest/Admin/Whatsanapp

Home app

Click the Splunk logo to return to the app that was set as your default app; the default is the Home app



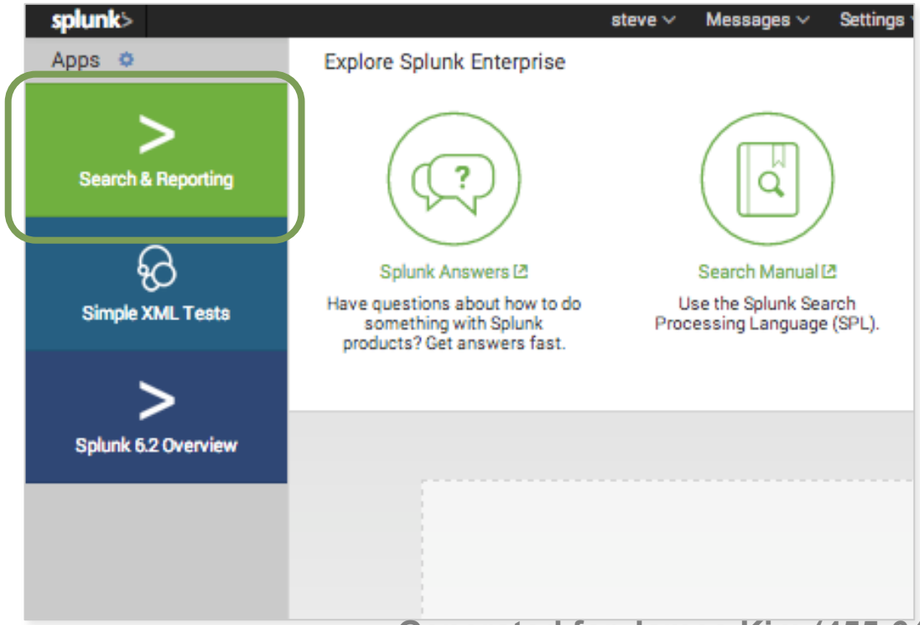
Links to several help resources

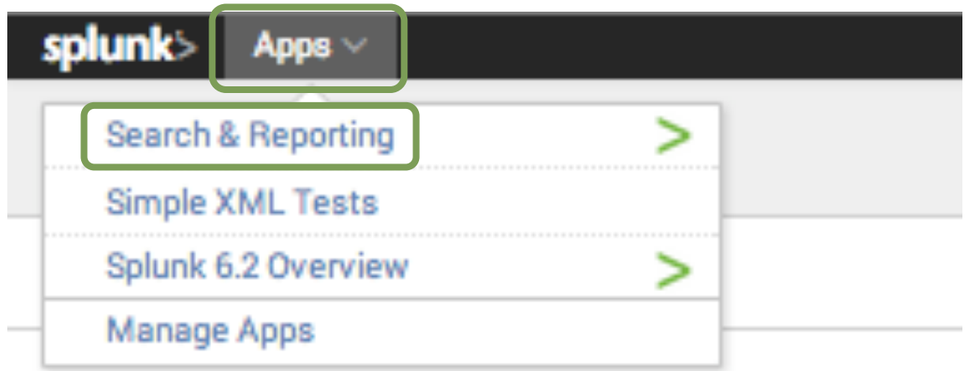
Select app context

Once you've built dashboards with your data, you can choose one to appear in your Home app

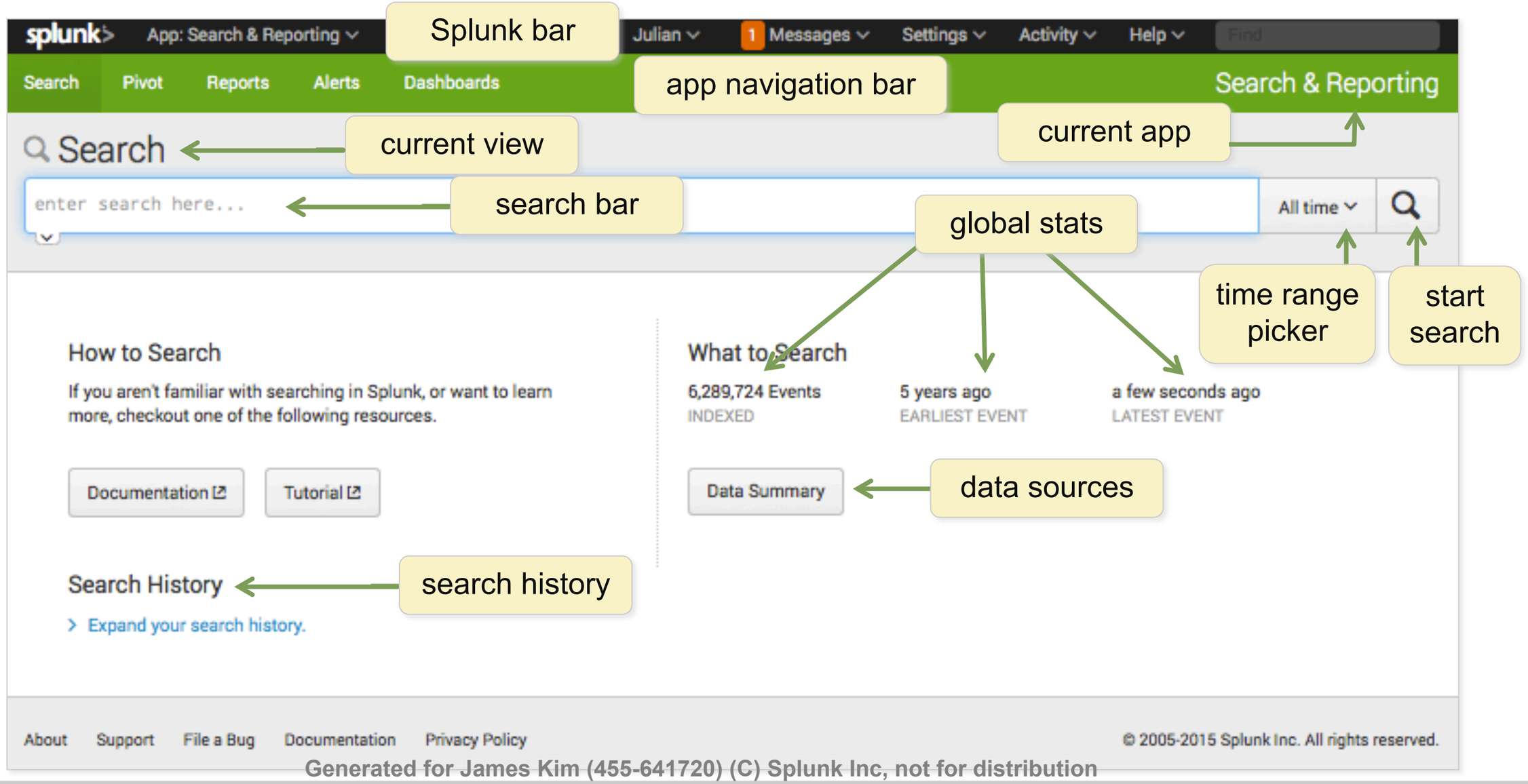
Search & Reporting App Overview

- Provides a default interface for searching and analyzing data
- Enables you to create knowledge objects, reports, and dashboards
- Access by selecting the **Search & Reporting** button on the Home view or, from an app view, select **Apps**, then select **Search & Reporting**

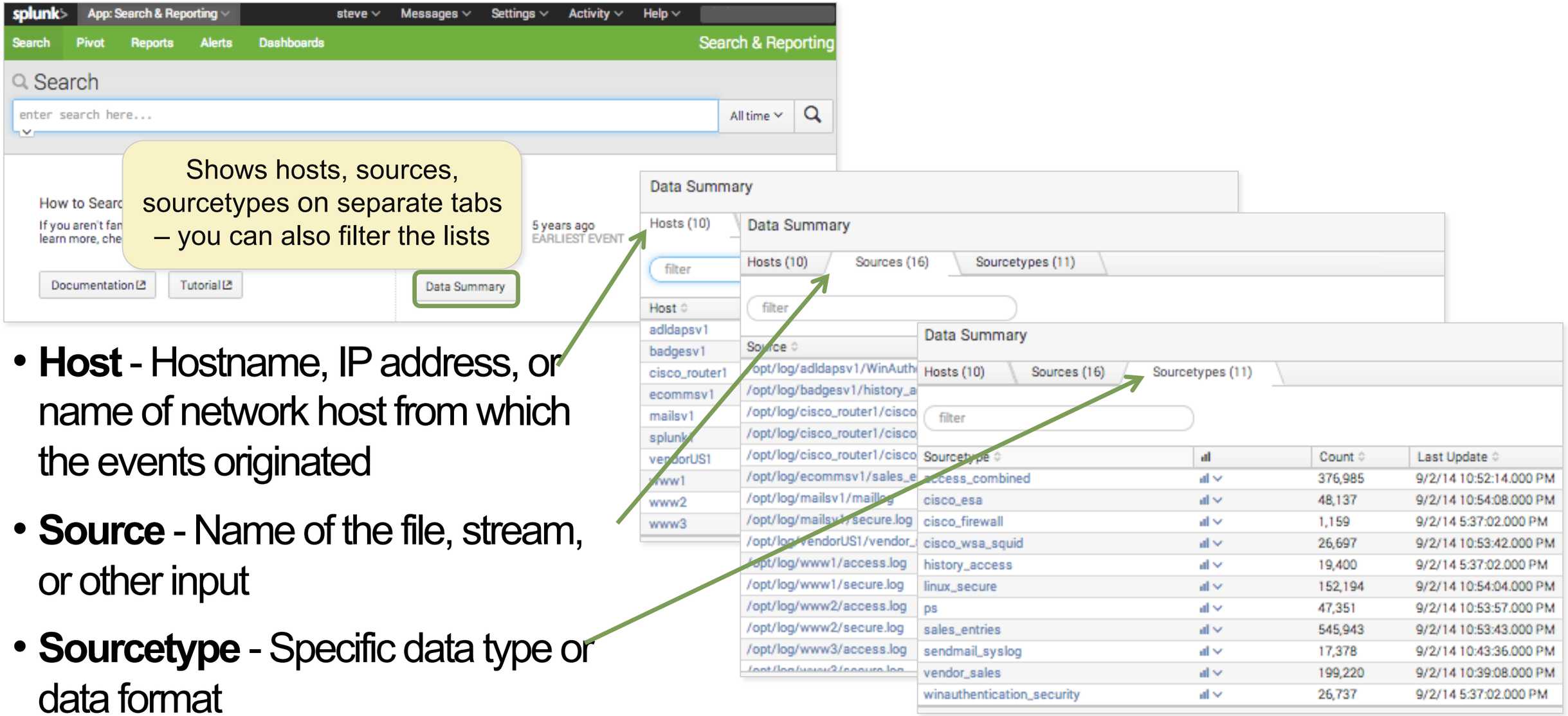




Search & Reporting App Overview (cont.)

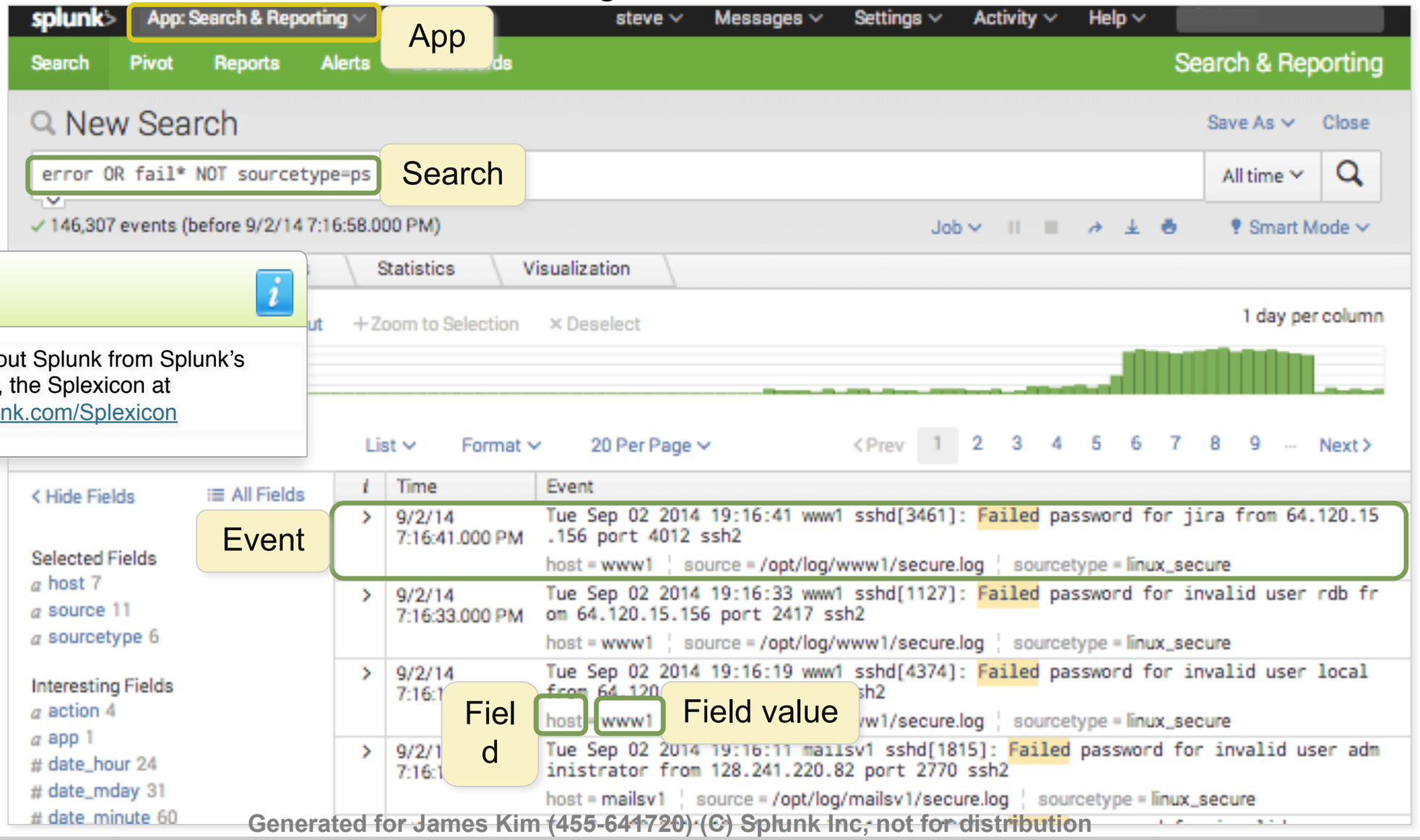


Data Summary Views



- **Host** - Hostname, IP address, or name of network host from which the events originated
- **Source** - Name of the file, stream, or other input
- **Sourcetype** - Specific data type or data format

Key Details



Note

Learn more about Splunk from Splunk's online glossary, the Splexicon at http://docs.splunk.com/Splexicon

Searching

Module Objectives

- Run basic searches
- Set the time range of a search
- Identify the contents of search results
- Refine searches
- Use the timeline
- Work with events
- Control a search job
- Save search results

Why Learn to Search?

- Why is it important to be able to write searches?
  - Every report and visualization is built based on an underlying search
  - Understanding, analyzing, and troubleshooting visualizations will depend on your ability to understand the search text
  - Mastering the search language will enable you to do as much as possible with your data to meet your specific needs

Everything is Searchable

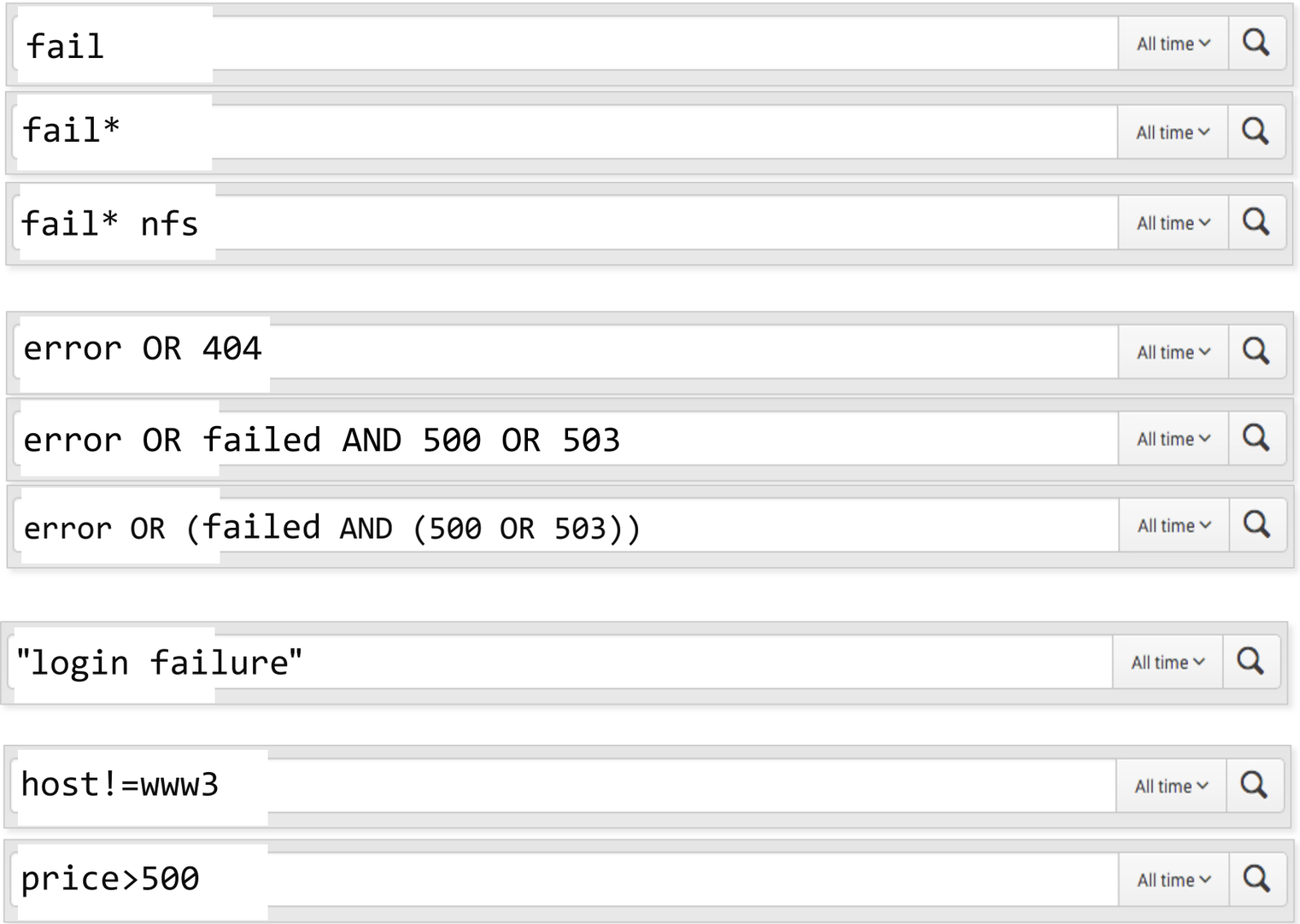
- * wildcard supported
- Search terms are case **in**sensitive
- Booleans AND, OR, NOT
  - Must be uppercase
  - AND is implied between terms
  - Use () for complex searches
- Quotation marks for phrases
- Relationship specifiers

  != means does not equal

  = means is equal to

  < means is less than

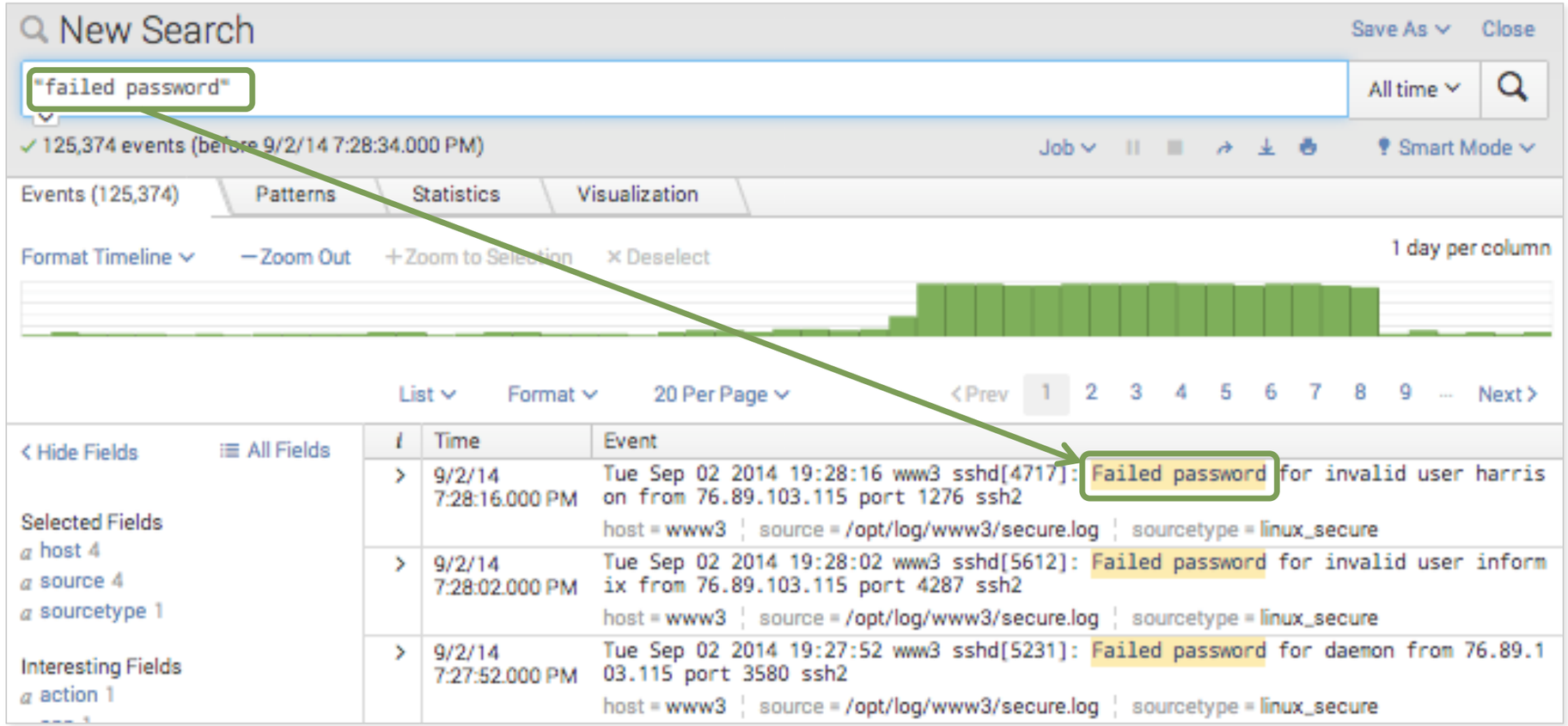
  > means is greater than



Search Results

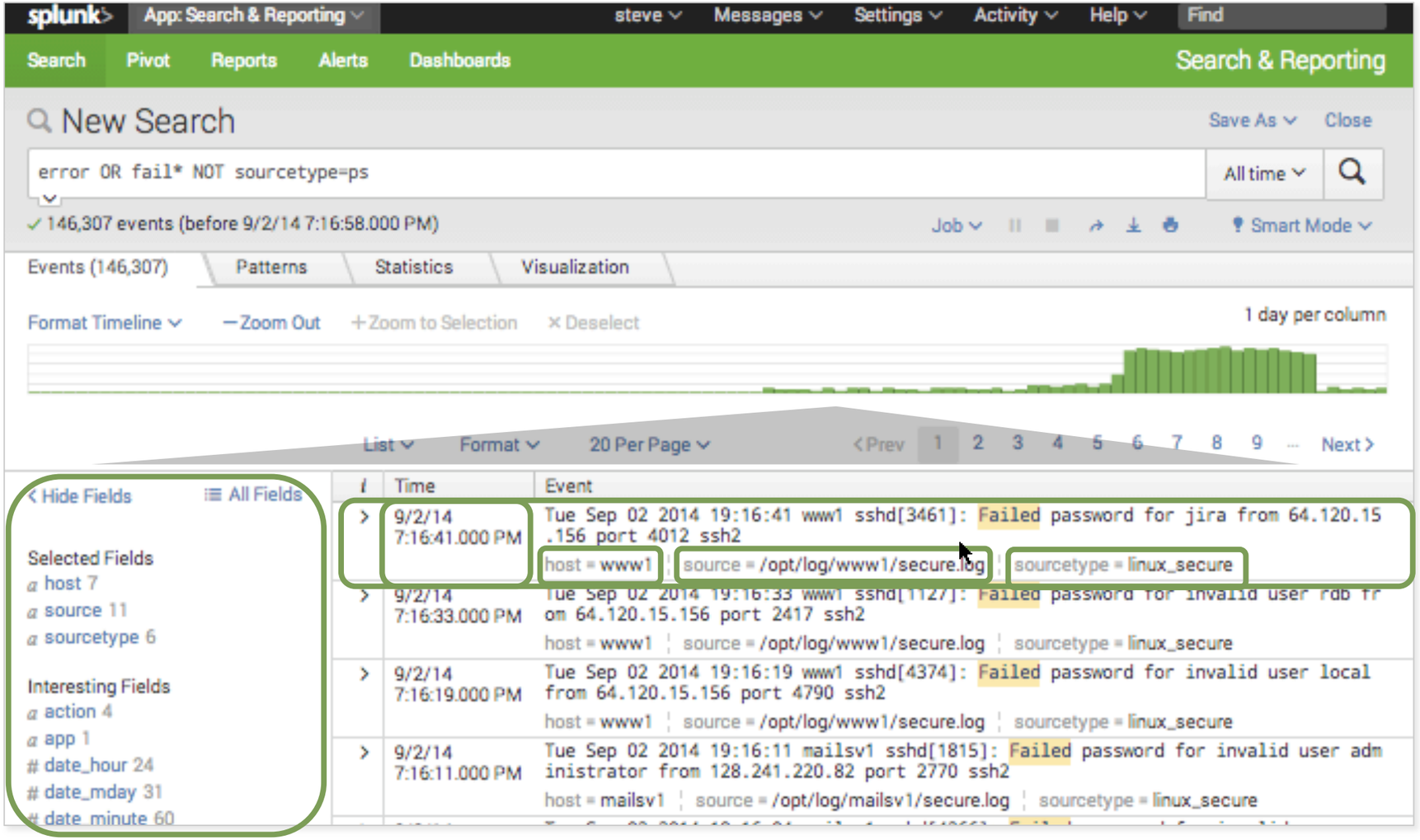
Matching results are returned immediately

- Displayed in reverse chronological order (newest first)
- Matching search terms are highlighted



Event Details

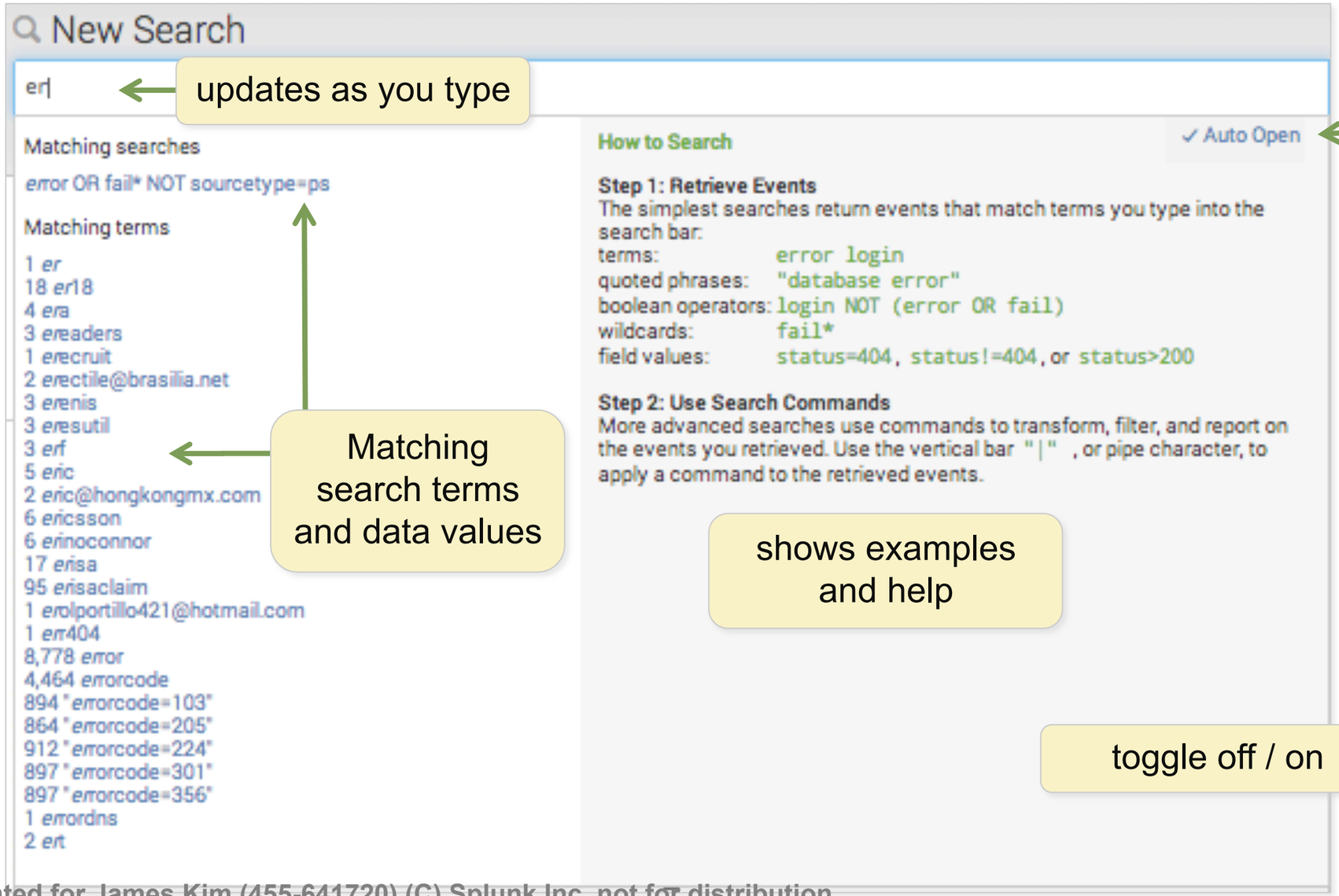
- Splunk parses data into individual events
- Each event has a
  - timestamp
  - Host
  - source
  - sourcetype
- Fields are also listed in the Fields sidebar



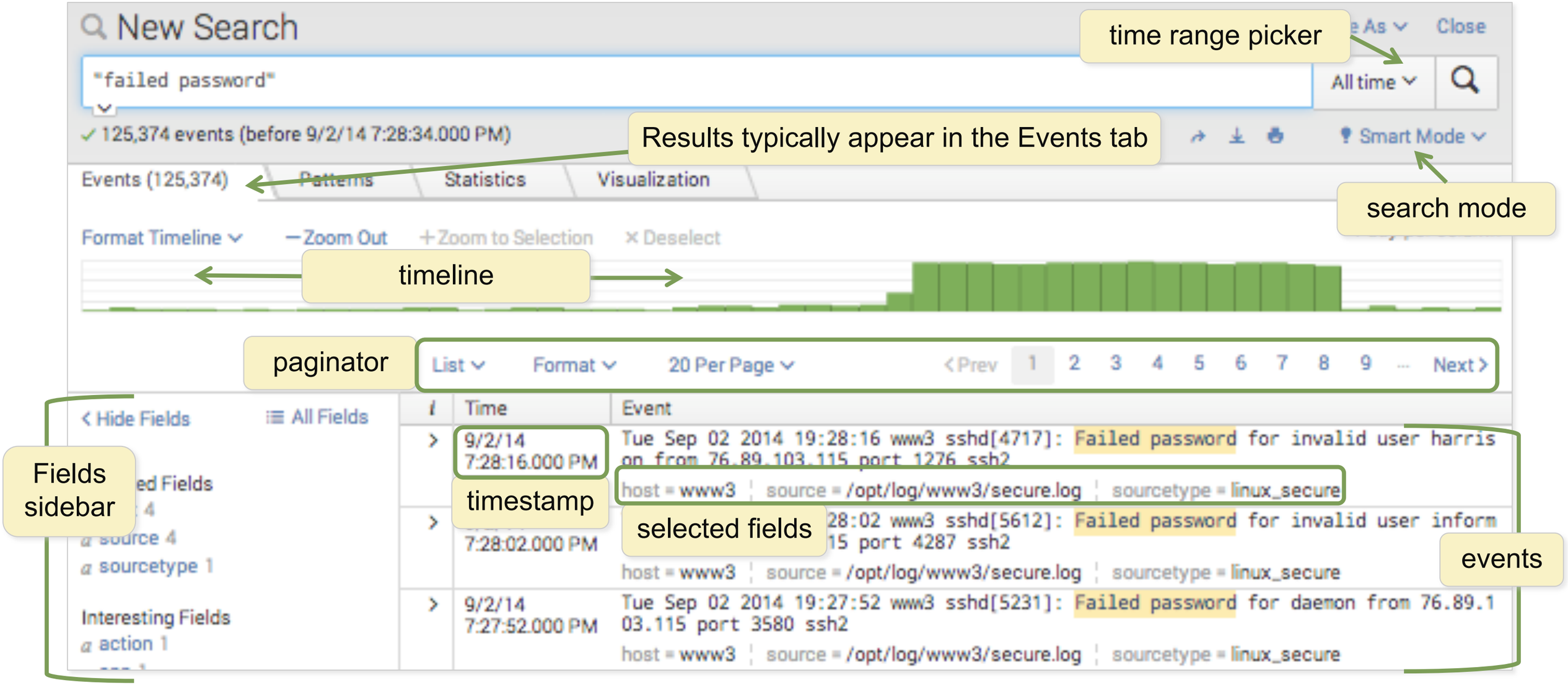
Search Assistant

Quick reference for Splunk search language that updates as you type and shows:

- matching searches
- matching terms
- examples
- links to documentation when using commands

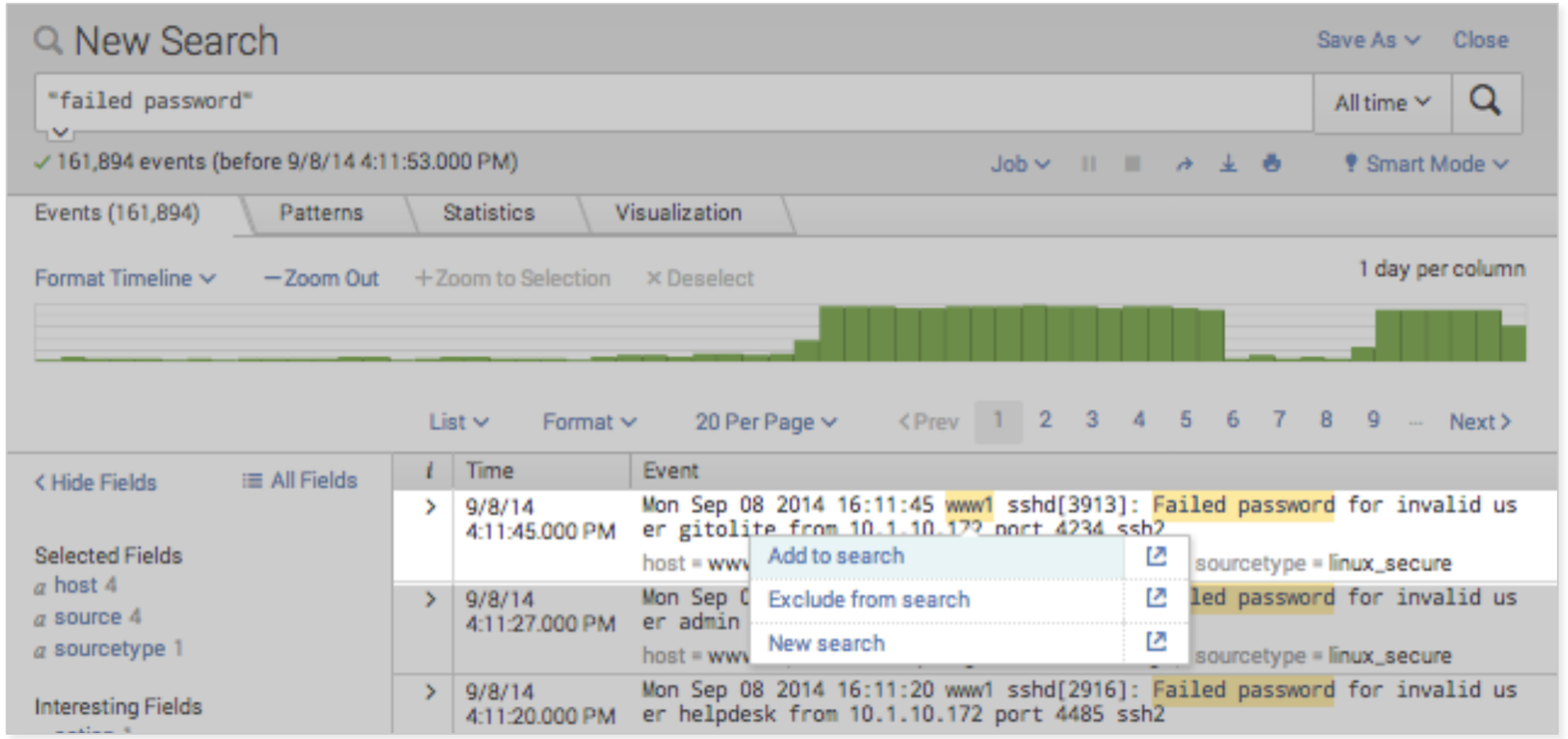


Search Results Details



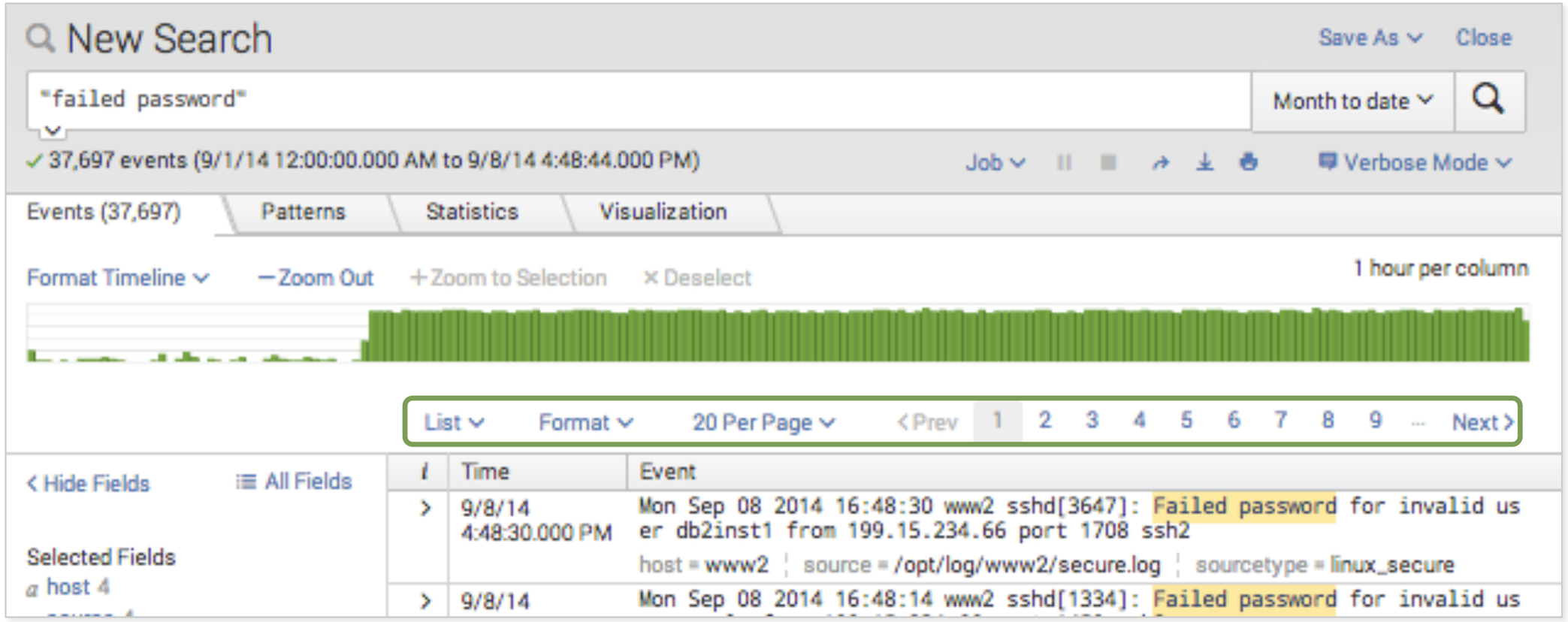
Use Search Results to Modify a Search

- When you mouse over search results, keywords and parts of keywords are highlighted
- Click any item in your search results. A window appears allowing you to add it to the search, exclude it from the search, or open a new search including only that item

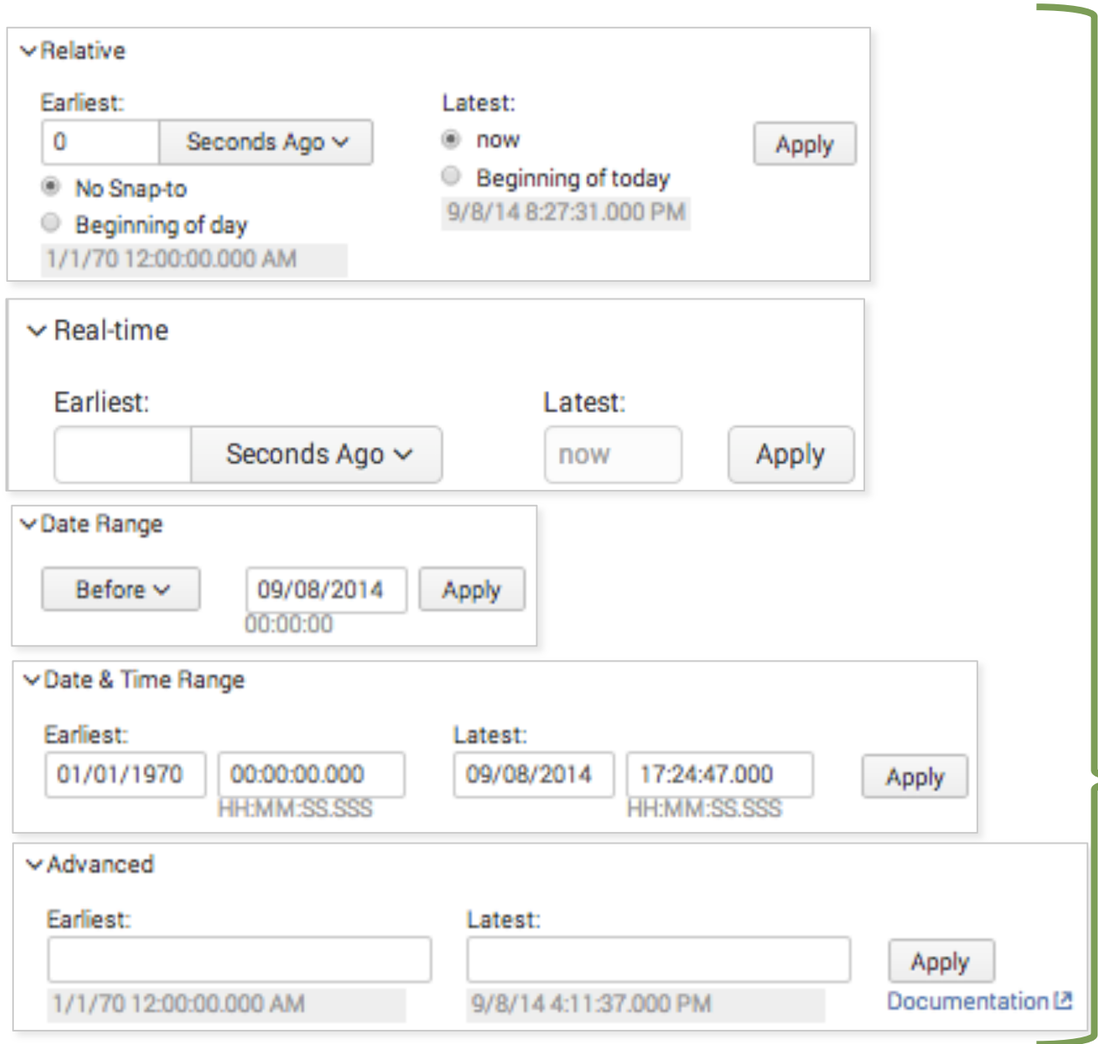


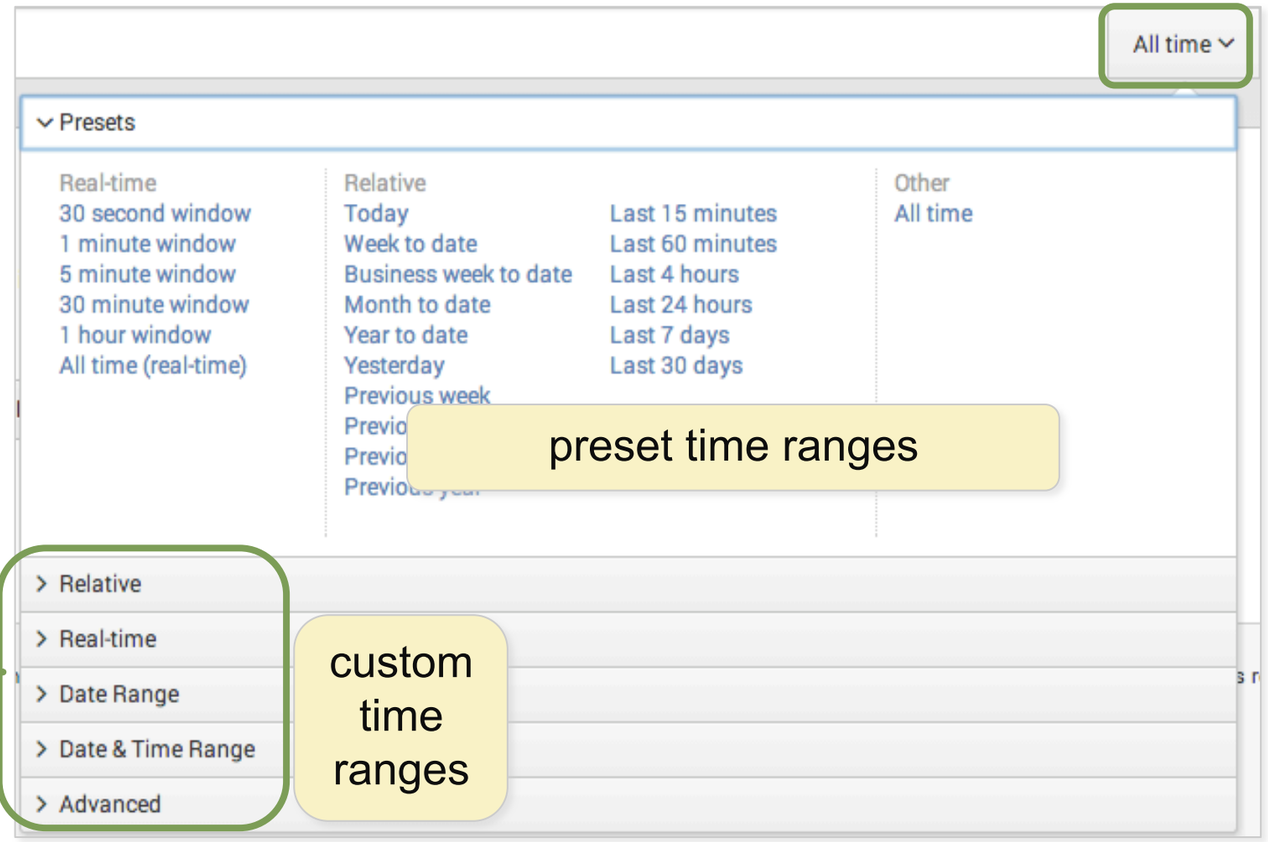
Change Search Results View Options

If you prefer a different layout for displaying your search results, in each tab you can select your own view options



Select a Specific Time





Time Range Abbreviations

Time range is automatically populated with time setting of your search

Use abbreviations for time range syntax:

s=seconds m=minutes h=hours d=days w=week mon=months y=year

- @ symbol "snaps" to time unit you specify
  - Example: Current time when the search starts is 09:37:12

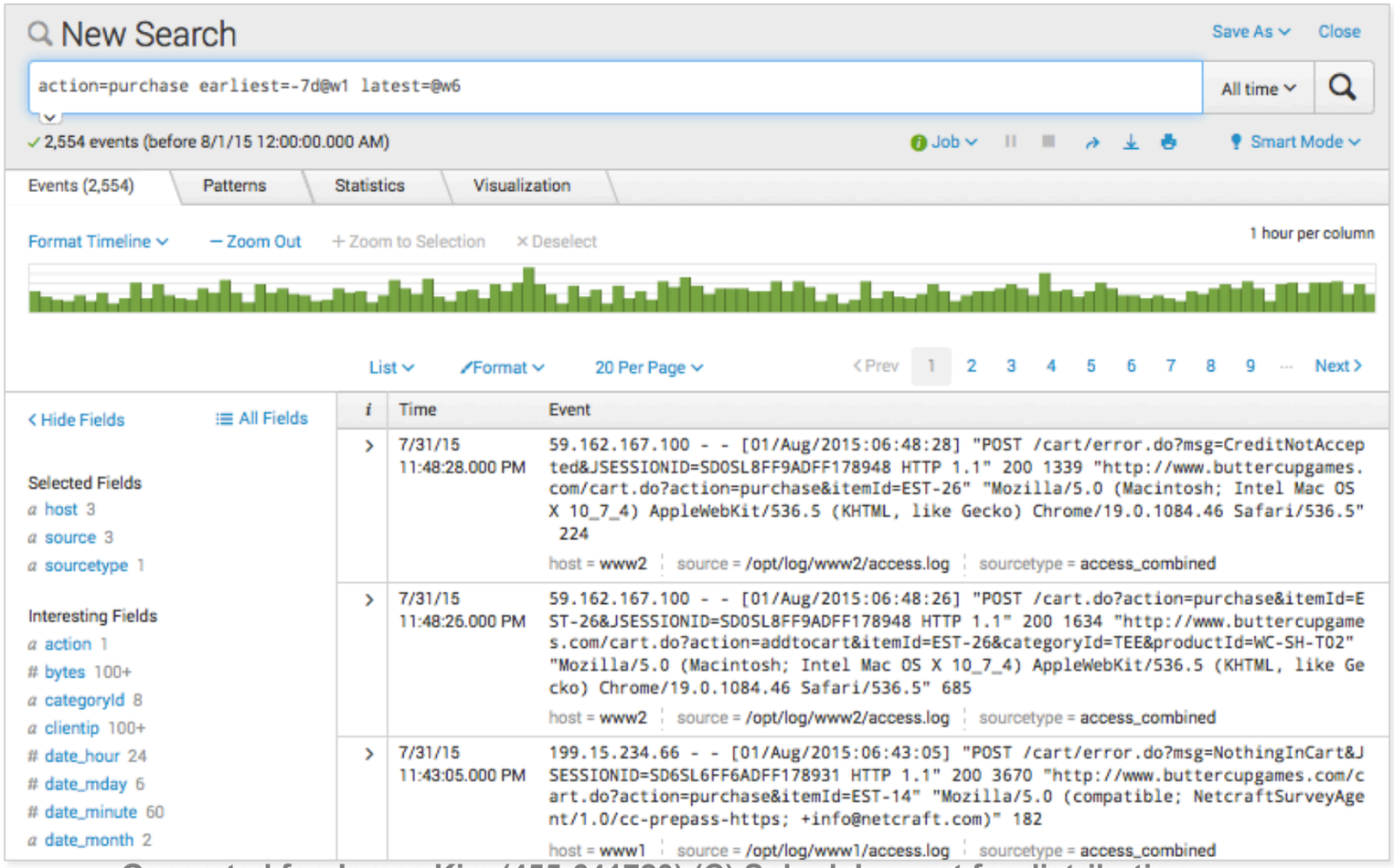
-5m	looks back to 09:32:12
-5m@m	looks back to 09:32:00
-30m@h	looks back to 09:00:00

- Earliest and latest

earliest=-h	looks back one hour
earliest=-7d@w1 latest=@w6	looks back one full week

Specifying Time in Search Text

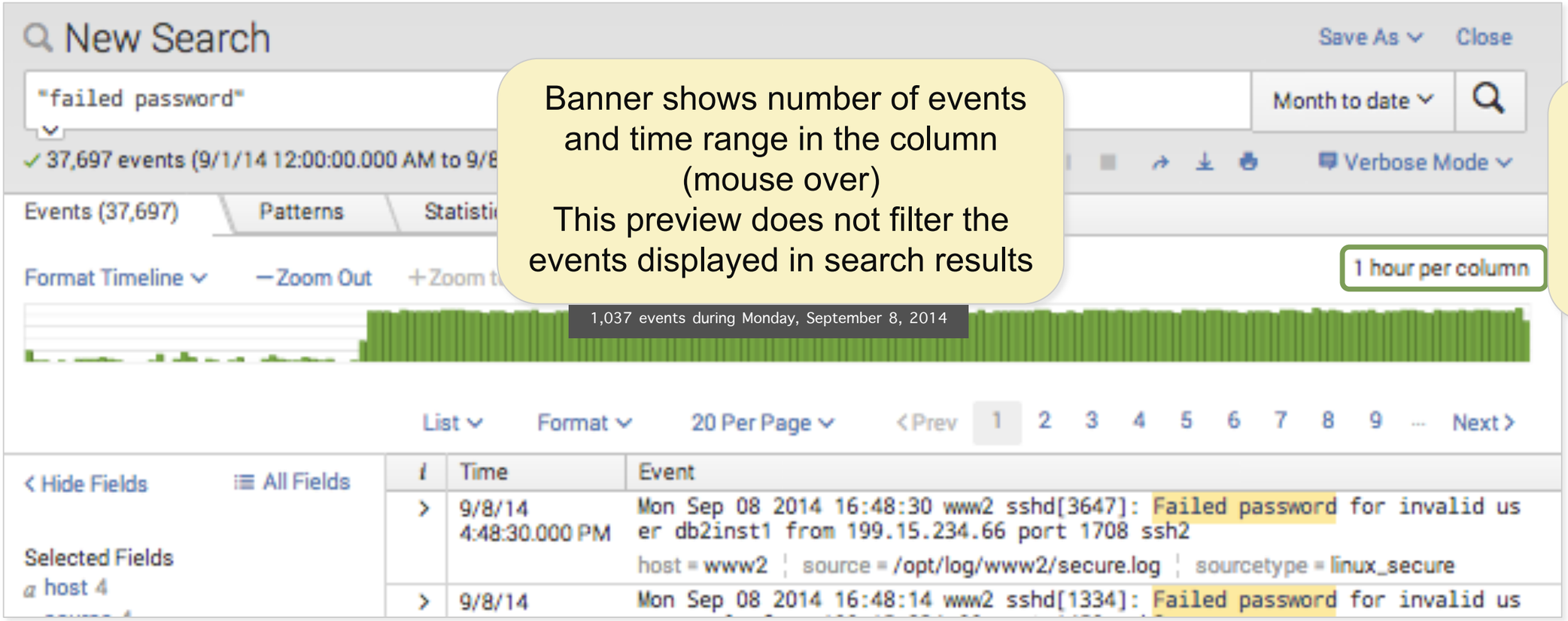
You can specify time range by using time abbreviations in your search text



View the Timeline

Timeline shows distribution of events the time range specified in the search

- Mouse over for details, or single-click to filter to results for that time period

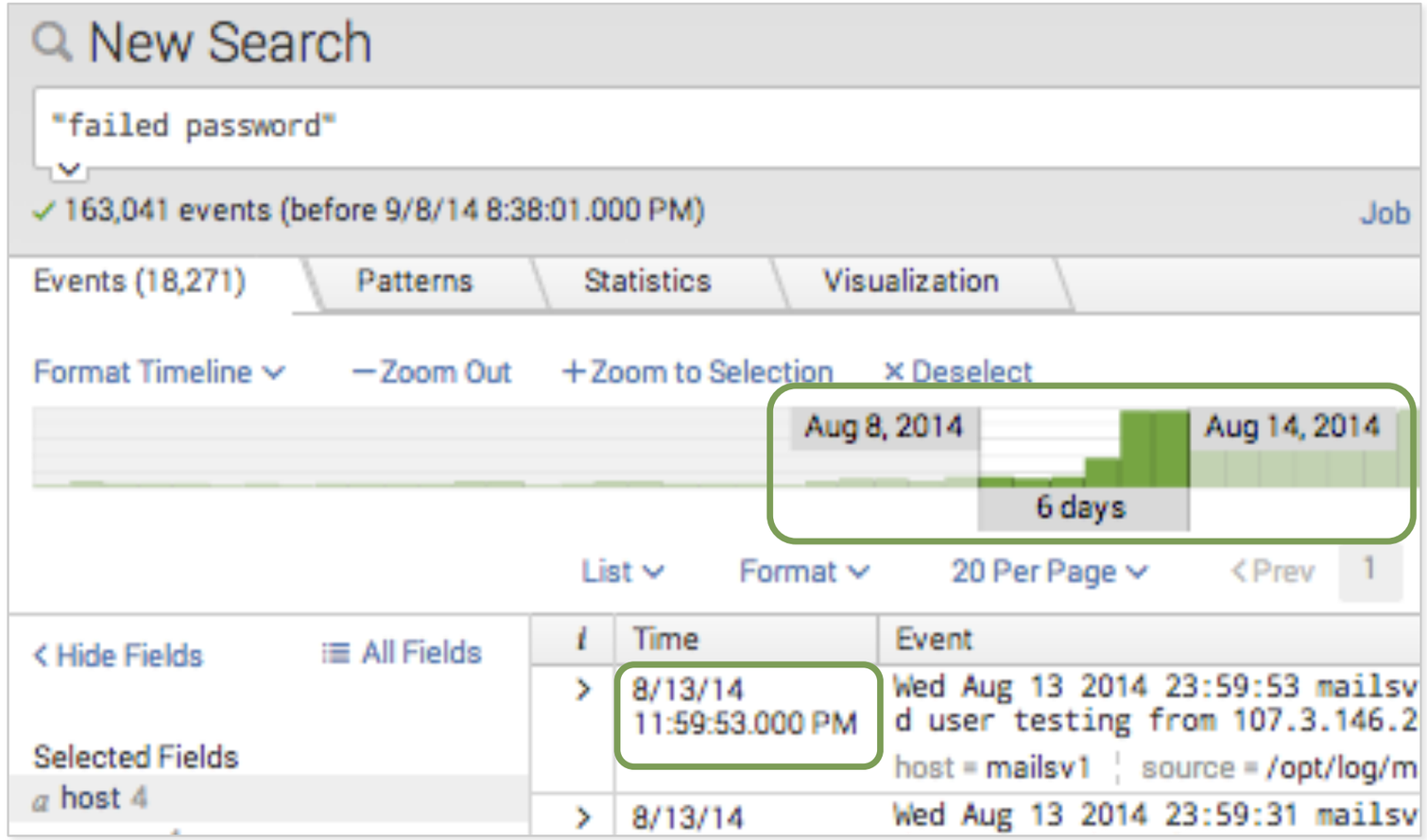


Banner shows number of events and time range in the column (mouse over)
This preview does not filter the events displayed in search results

Timeline legend shows the scale of the timeline

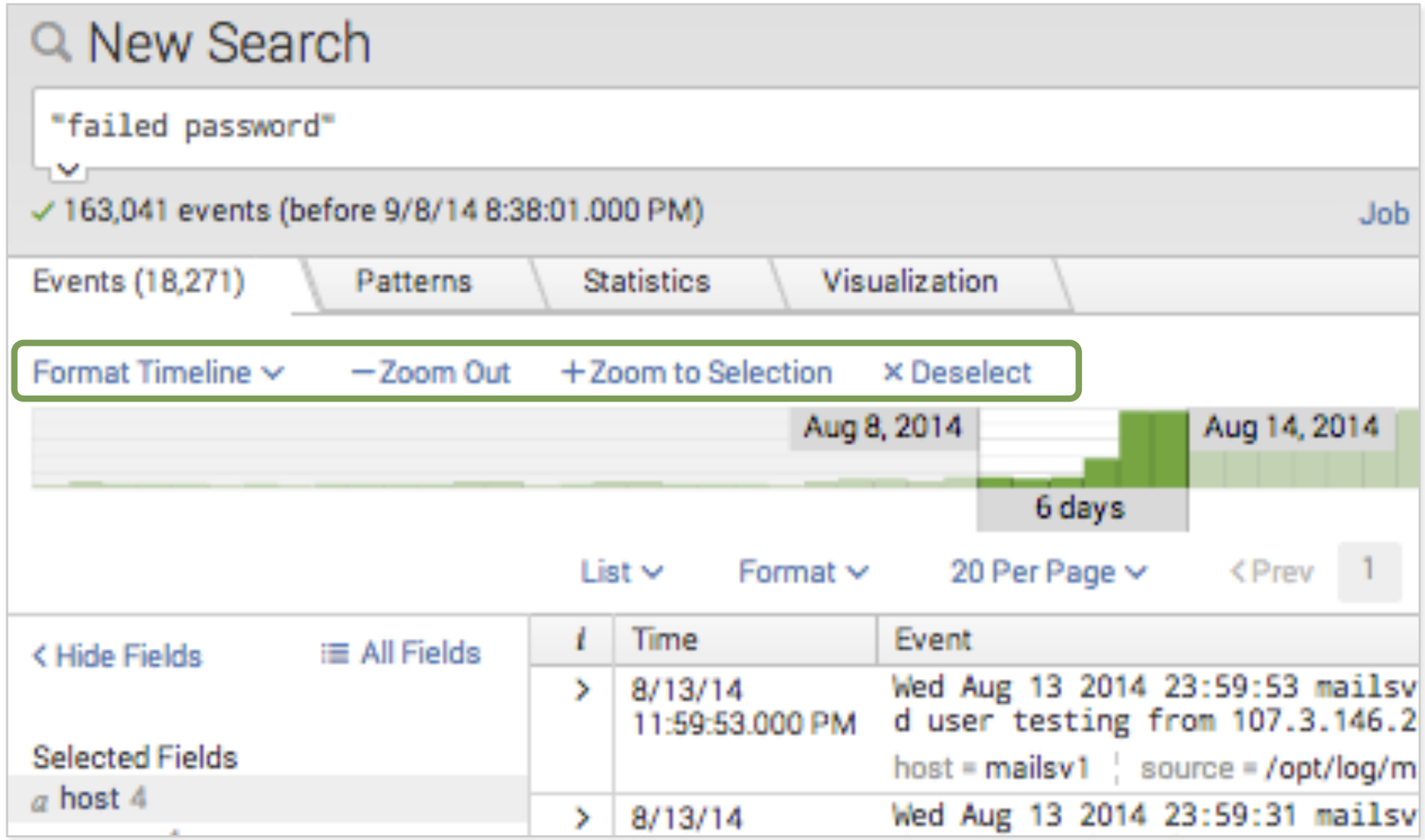
View a Subset of the Results with Timeline

- To select a narrower time range, click and drag across a series of bars
- This action filters the current search results
  - does not re-run the search
- Results are displayed in reverse chronological order (most recent first)



Use Other Timeline Controls

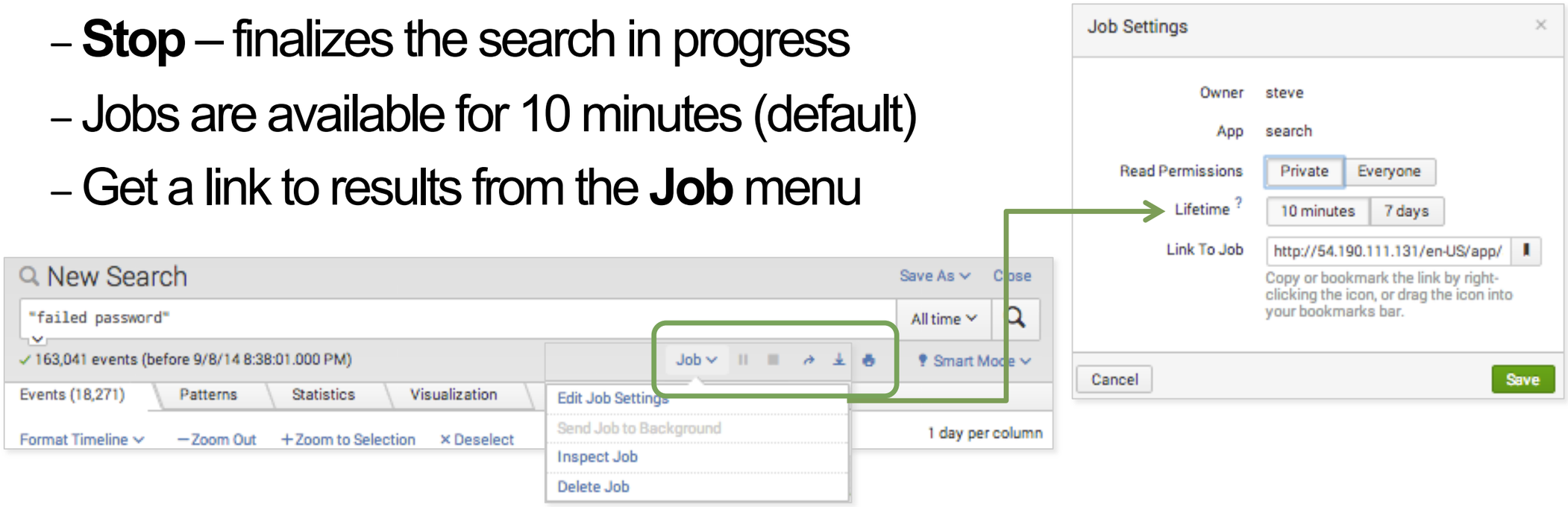
- **Format Timeline**
  - Hides or shows the timeline in different views
- **Zoom Out**
  - Expands the time focus & re-runs the search
- **Zoom to Selection**
  - Narrows the time range & re-runs the search
- **Deselect**
  - If in a drill down, returns to the original results set
  - Otherwise, grayed out / unavailable



Control or Save Search Jobs

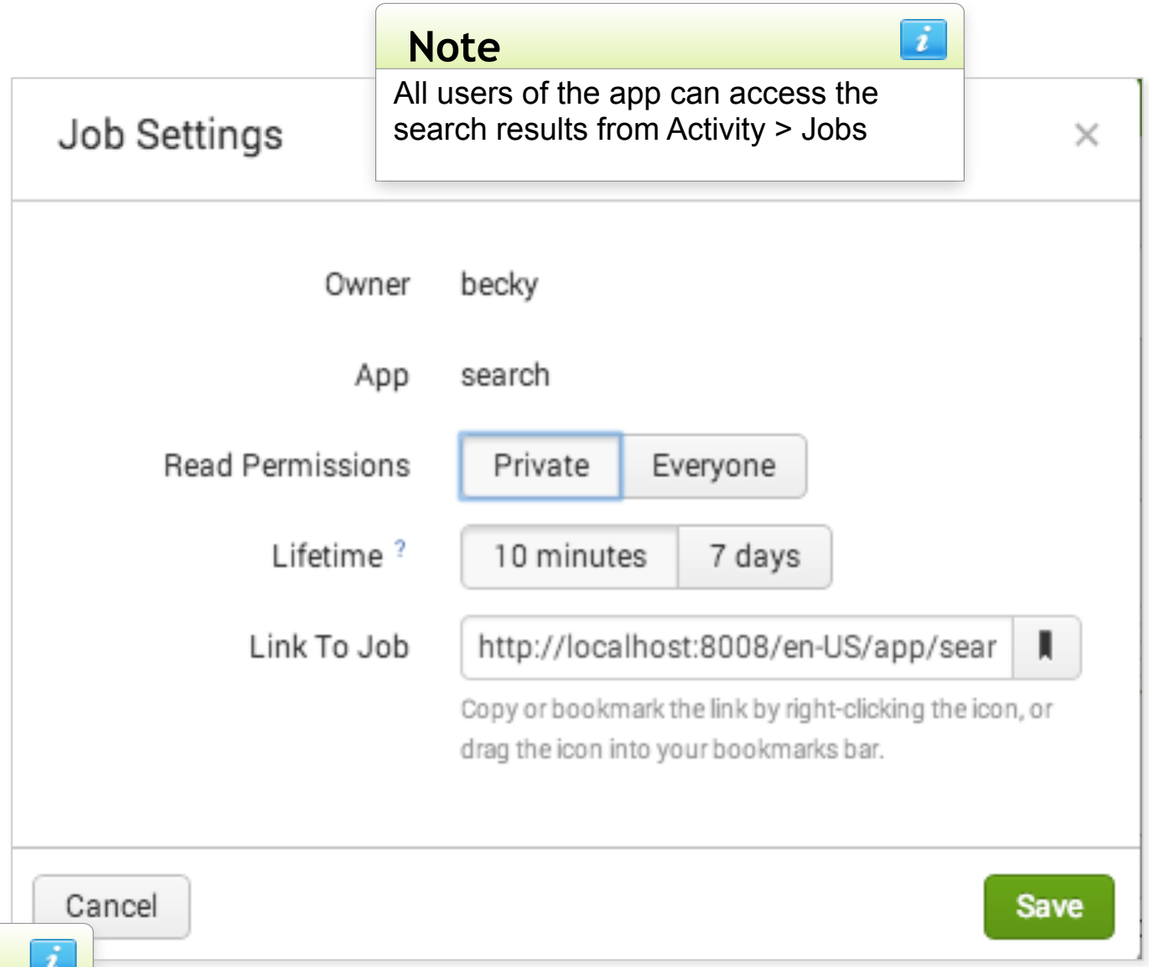
Every search is a **job.** The Job bar displays the progress of the search job (blue part of the bar represents the amount of the job that is complete)

- **Pause** – toggles to resume the search
- **Stop** – finalizes the search in progress
- Jobs are available for 10 minutes (default)
- Get a link to results from the **Job** menu



Set Permissions

- **Private** [default]
  - Only the creator can access
- **Everyone**
  - (All Search app users can access the search results)
- **Lifetime**
  - Default is 10 minutes
  - Can be extended to 7 days
  - To keep your search longer, schedule a report

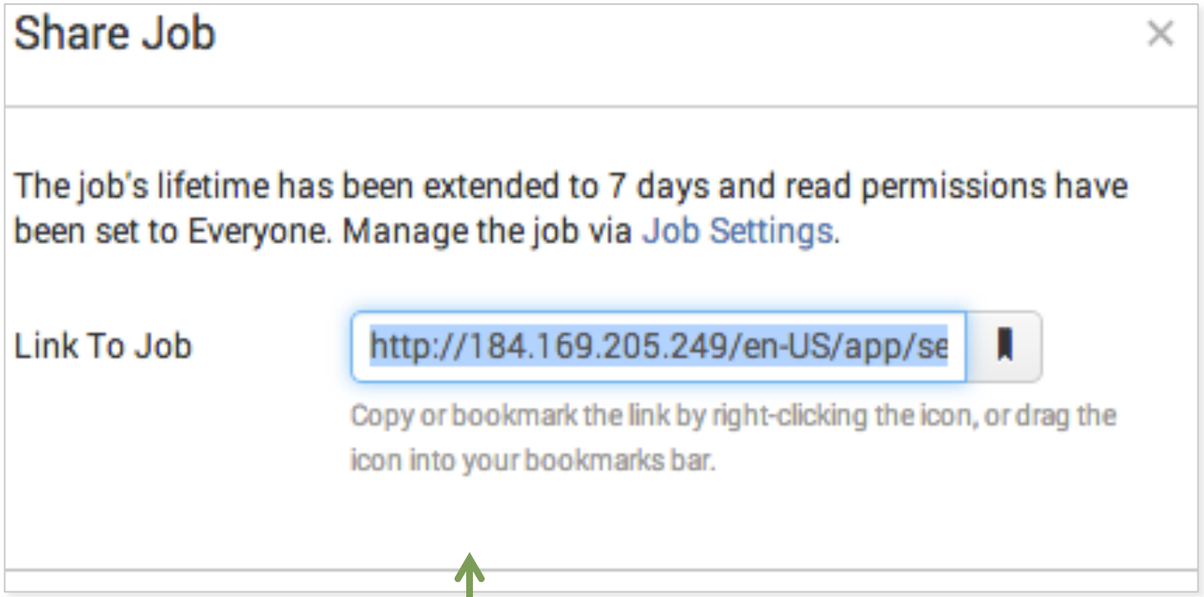


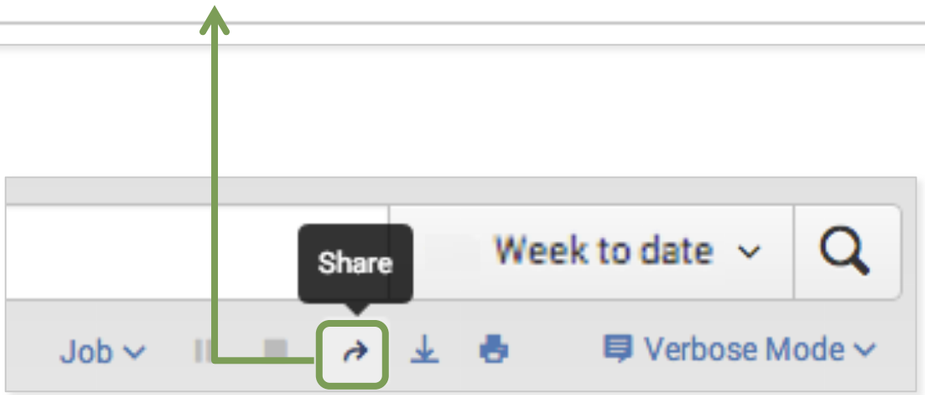
Note

Scheduled reports is covered in the Creating Knowledge Objects course.

Share Search Jobs

- Use the Share button next to the Job bar to quickly:
  - Apply read permissions to everyone
  - Extend the retention of the results to 7 days
  - Get a sharable link to the results
- Click the printer icon to print results or save them as PDF



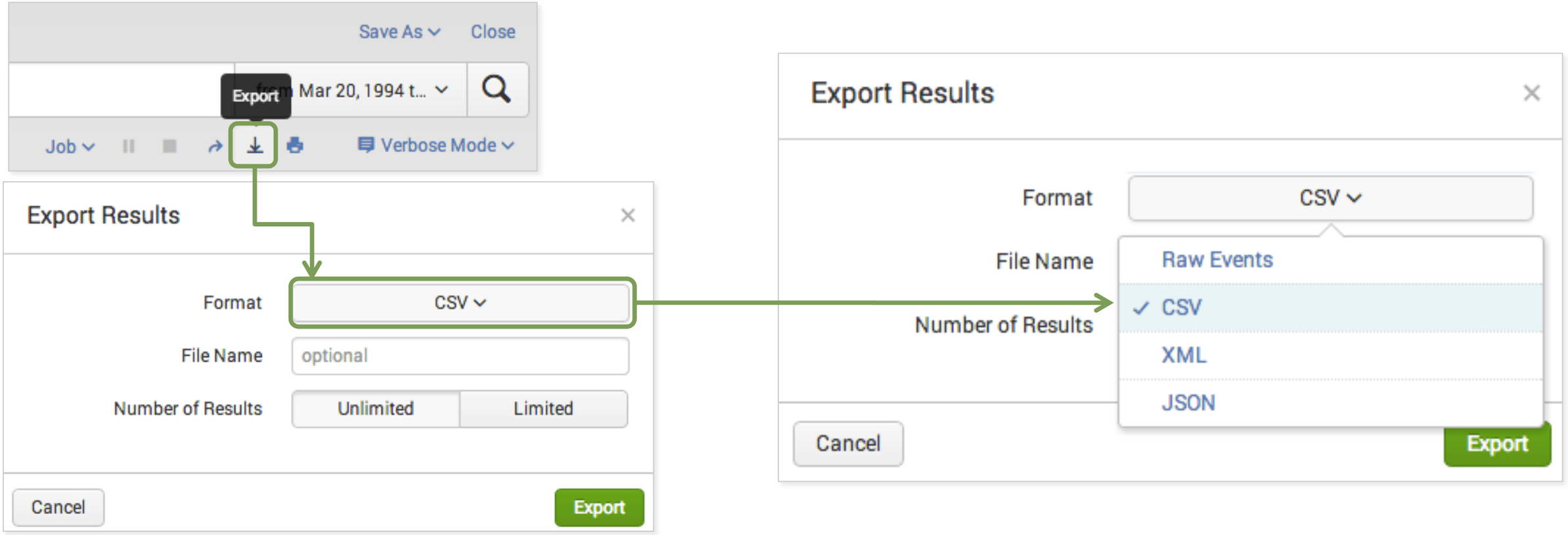


Note

Saving and sharing the actual search strings for reuse (known as **Reports**) is discussed later in this course.

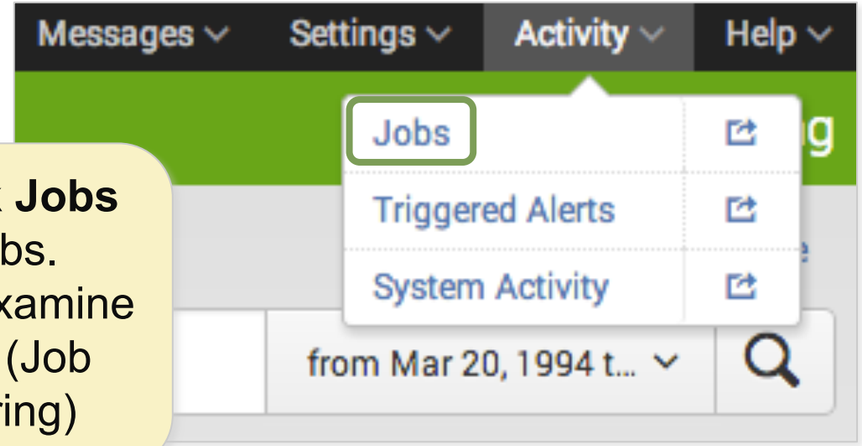
Export Search Results

For an external copy of the results, **export** search results to Raw Events (text file), CSV, XML, or JSON format

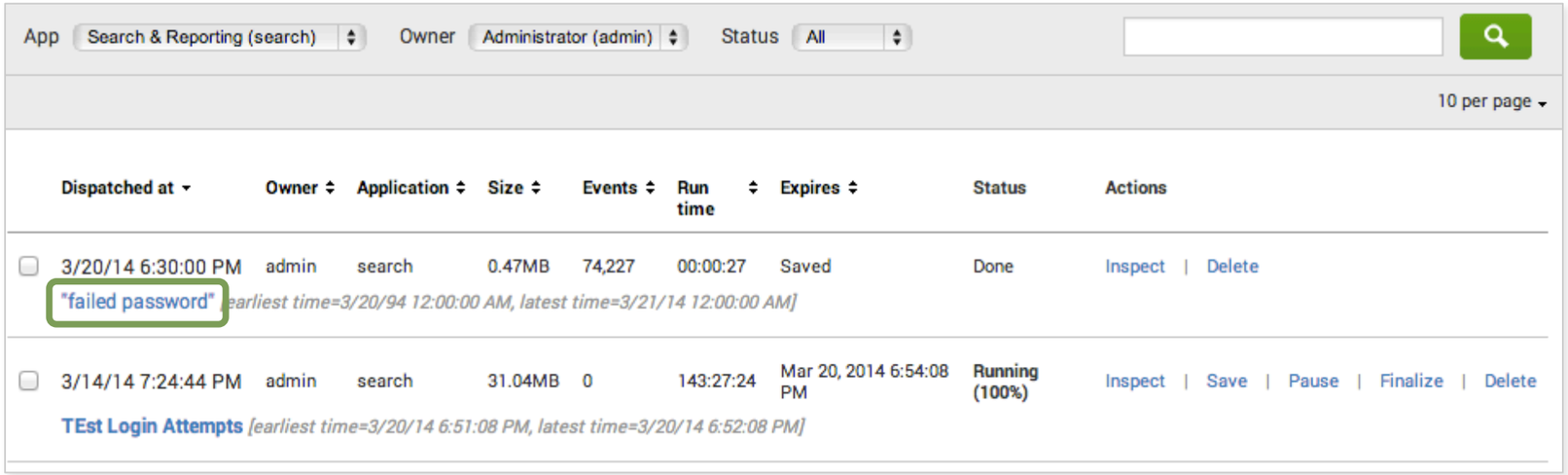


Review your Job History

- Access saved search jobs from the **Activity** menu
- The Search Jobs page displays jobs that:
  - You have run in the last 10 minutes
  - You have extended for 7 days
- Click on a job link to view the results in the Search view

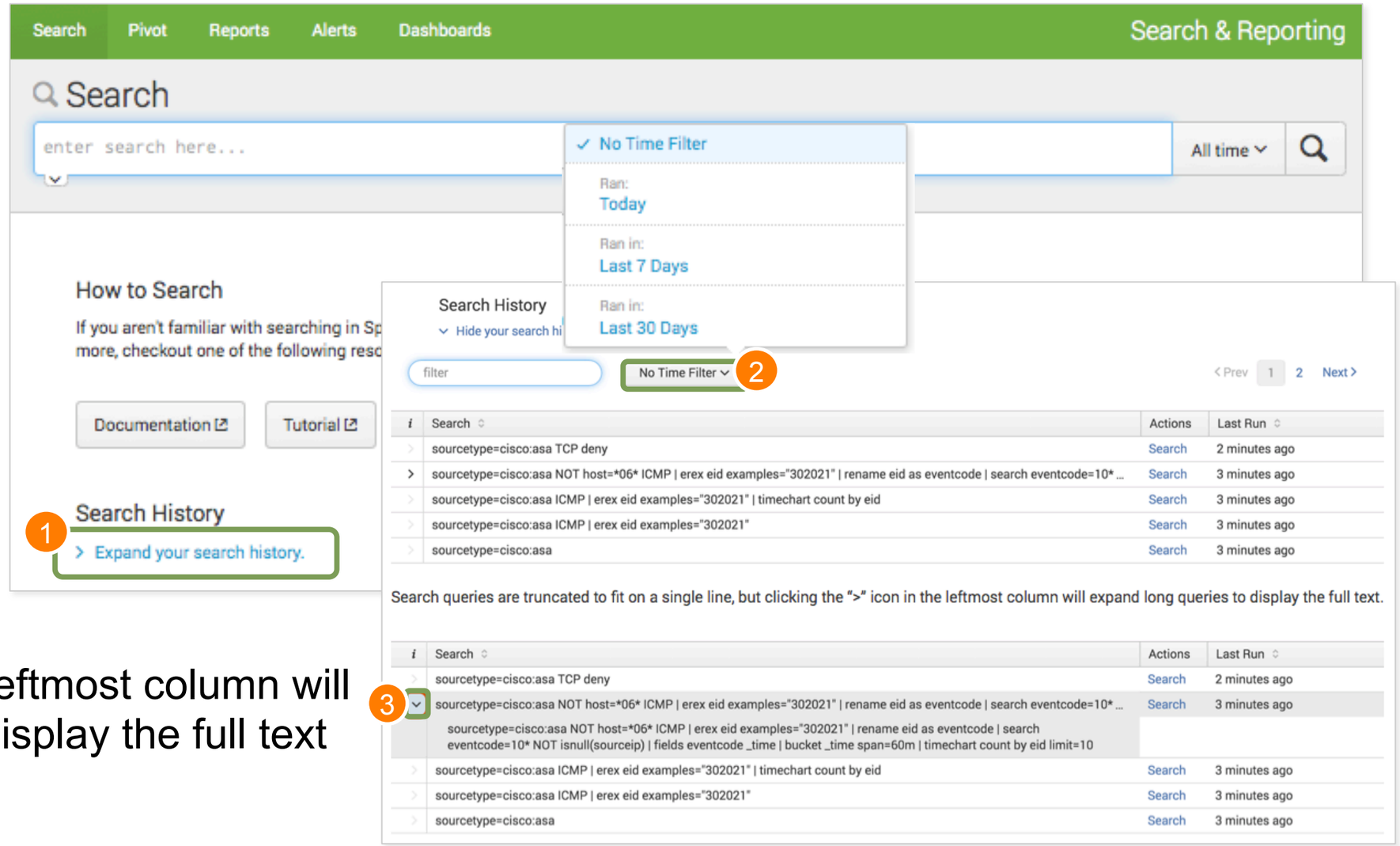


Click **Activity**, then click **Jobs** to view your saved jobs. Click the job's name to examine results in Search view. (Job name is the search string)



Review your Search History

1. Search History will display your 5 most recent ad-hoc search queries, truncated to fit on a single line
2. You can set a time filter to further narrow your results
3. Click the “>” icon in the leftmost column will expand long queries to display the full text



Using Fields in Searches

Module Objectives

- Understand fields
- Use fields in searches
- Use the fields sidebar
- Use search modes (fast, verbose, and smart)

What are Fields?

- Fields are searchable key/value pairs in your event data
  - Example: host=www1, status=503
- All fields have names (host and status in the examples above) and can be searched with those names, like separating an http status code of 404 from Atlanta's area code

Boolean Examples with Fields

- `sourcetype=access_combined OR sourcetype=linux_secure`
- `host=www* login failed NOT invalid`
- `sourcetype=linux_secure failed NOT (admin OR root OR administrator)`
- `index=_internal NOT log_level=INFO sourcetype=dhcplogs (dest!=Prefix1* OR dest!=Prefix2*)`

Field Discovery

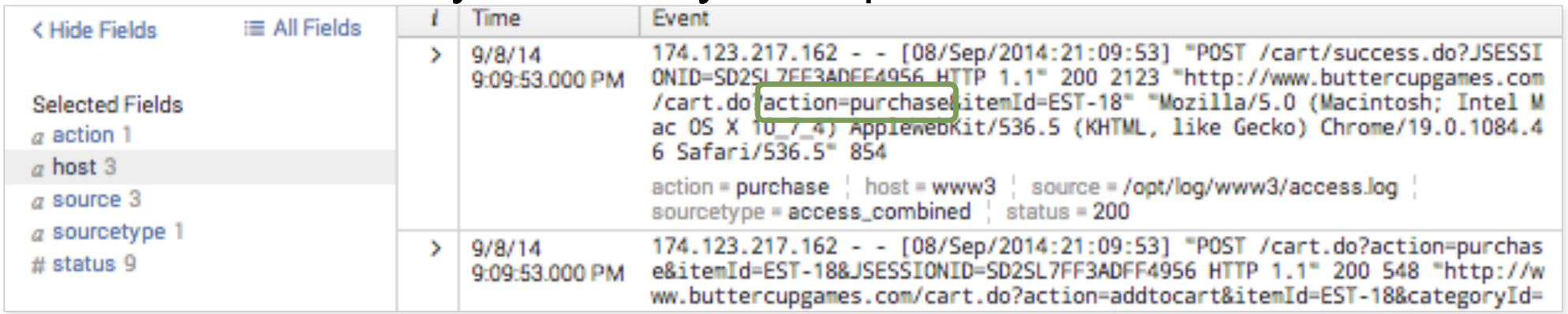
- Splunk discovers all fields based on sourcetype and any key/value pairs found in the data.
- Already stored with the event in the index (prior to search time) are:
  - Default fields, such as **host**, **source**, and **sourcetype**
  - Internal fields like **_time**, **_raw**
  - Splunk also extracts other fields in the event data that are not directly related to the search
- **Field discovery** is directly related to each search's results
  - Based on the search mode, Splunk will display more or fewer fields
  - Some fields that appear in the overall data may not exist within the results of some searches

Note

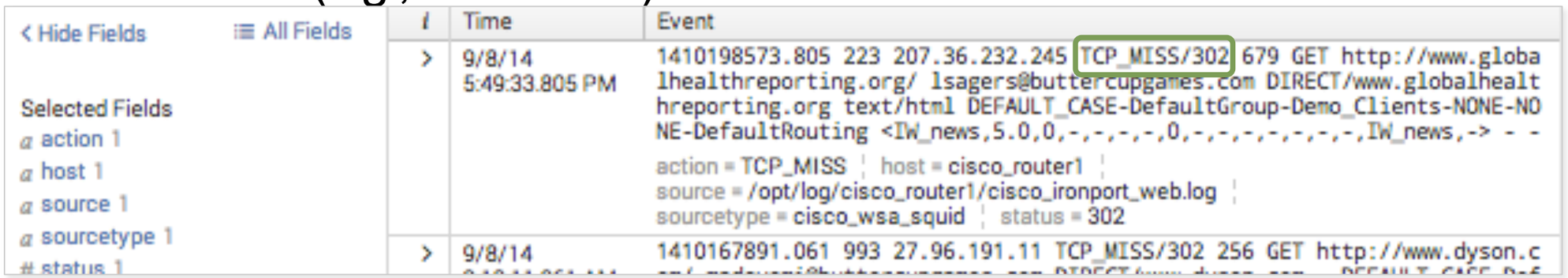
While Splunk auto-extracts many fields, you can learn how to create your own in the *Searching and Reporting with Splunk* course.

Identify Data-Specific Fields

- Data-specific fields come from the specific characteristics of your data
  - Sometimes indicated by obvious key=value pairs



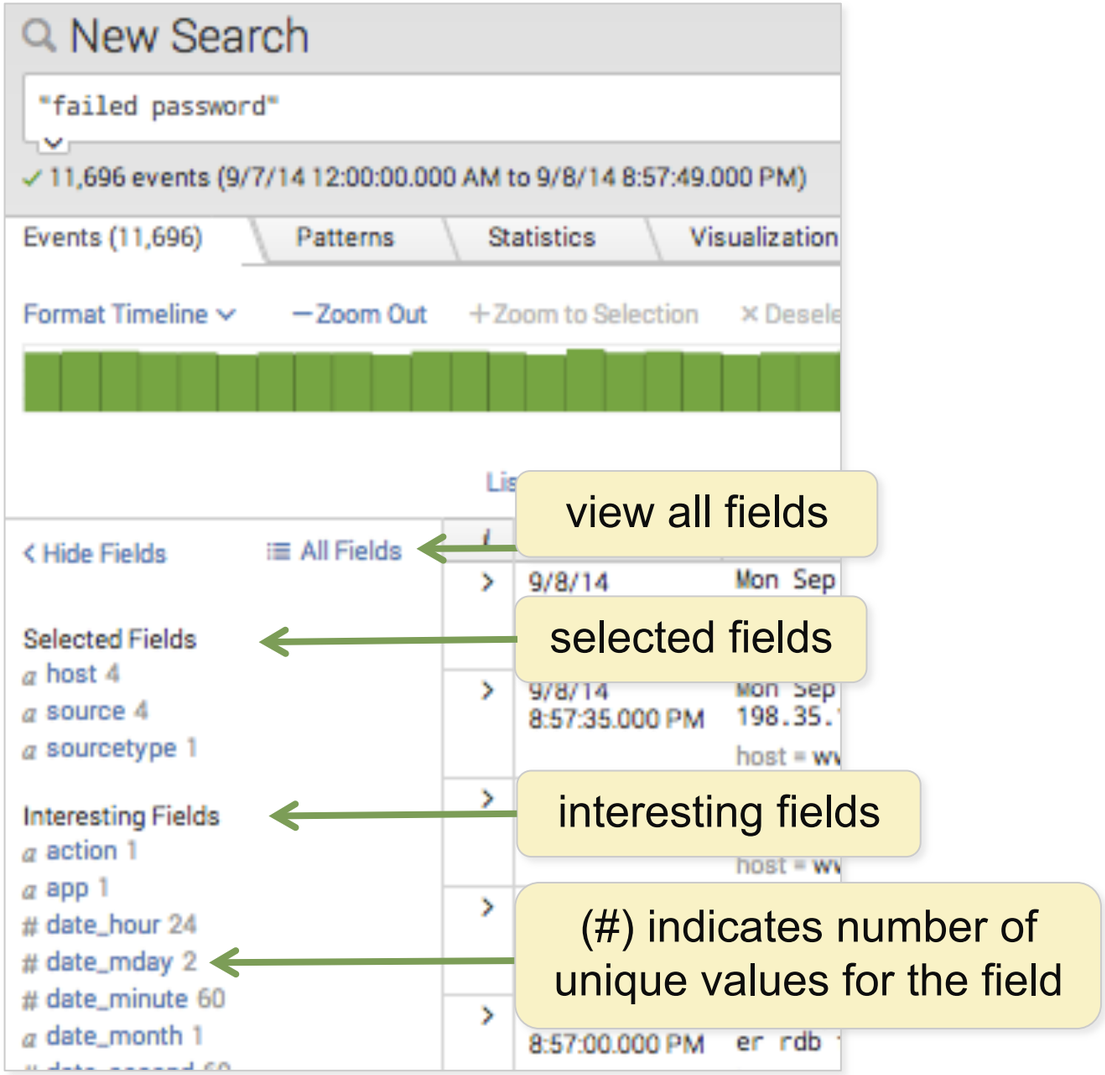
  - Sometimes not (e.g., status=302)



  - For more information, please see: http://docs.splunk.com/Documentation/Splunk/latest/Data/Listofpretrainedsourcetypes

Fields Sidebar

- For the current search, it shows
  - Selected fields
  - Interesting fields
  - Link to view all fields
- Splunk returns fields recognized from your search results
  - Interesting fields are those that have values in over 20% of events
  - Total fields vary depending on your search mode
  - The preceding # indicates the field's values are numeric



Use Fields in Searches

- Efficient way to pinpoint searches and refine results

```
141.146.8.66
```

```
clientip=141.146.8.66
```

```
status=404
```

```
area_code=404
```

- Field names ARE case sensitive, field values are NOT
  - Example:

```
host=www3
```

✓ 323 events 1/9/14 12:00:00.000 AM to

```
host=WWW3
```

✓ 323 events 1/9/14 12:00:00.000 AM to

These two searches return results

```
HOST=www3
```

✓ 0 events 1/9/14 12:00:00.000 AM to

This one does not return results

Use Fields in Searches (cont.)

- For IP fields, Splunk is subnet/CIDR aware

```
clientip="141.146.8.0/24"
```

```
clientip="141.146.8.*"
```

- Use wildcards to match a range of field values
  (user=* to display all events that contain a value for user)

```
user=* sourcetype=access* (referer_domain=*.cn OR referer_domain=*.hk)
```

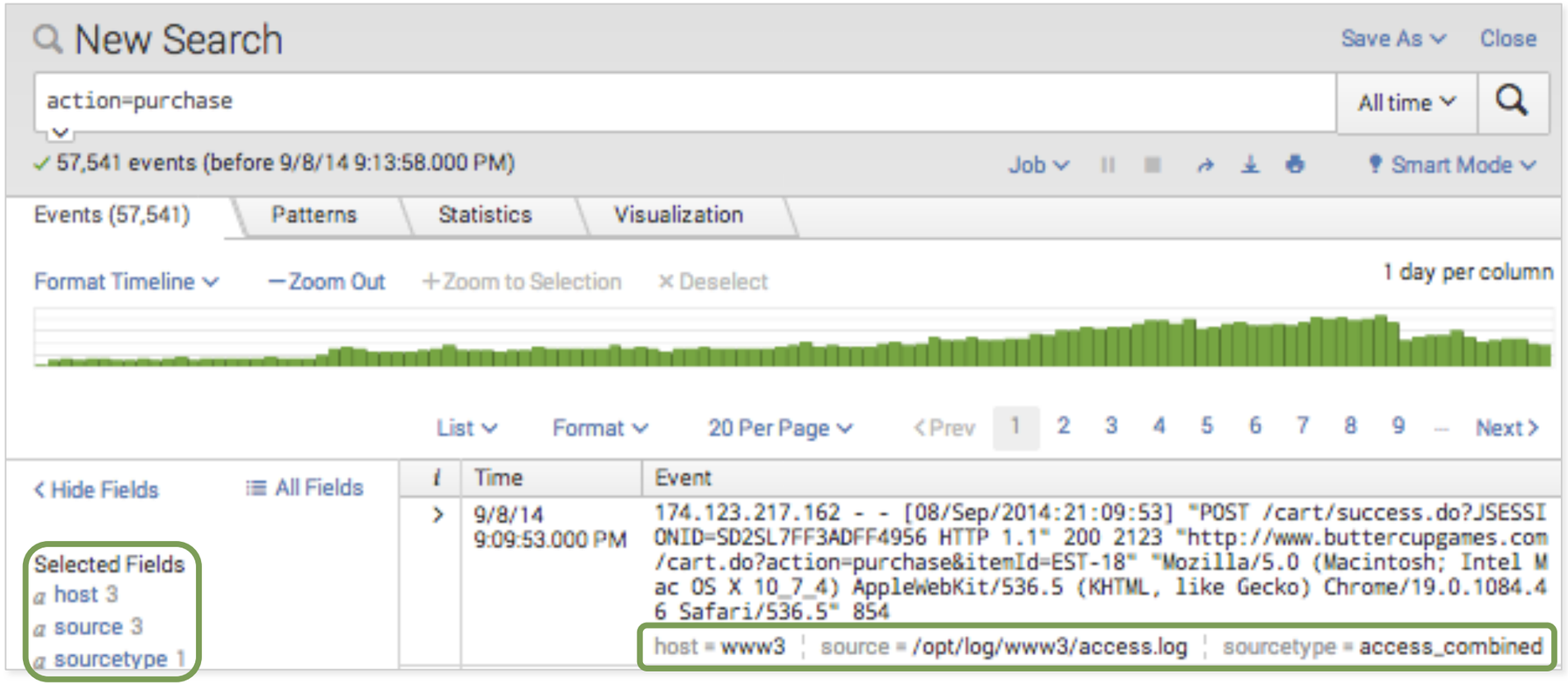
All time

- Use comparison operators for numeric field values

```
src_port>1000 src_port<4000
```

Describe Selected Fields

- Selected fields and their values are listed under every event that includes those fields.
- By default, the selected fields are:
  - host
  - source
  - sourcetype
- You can set a field to be selected in the future.



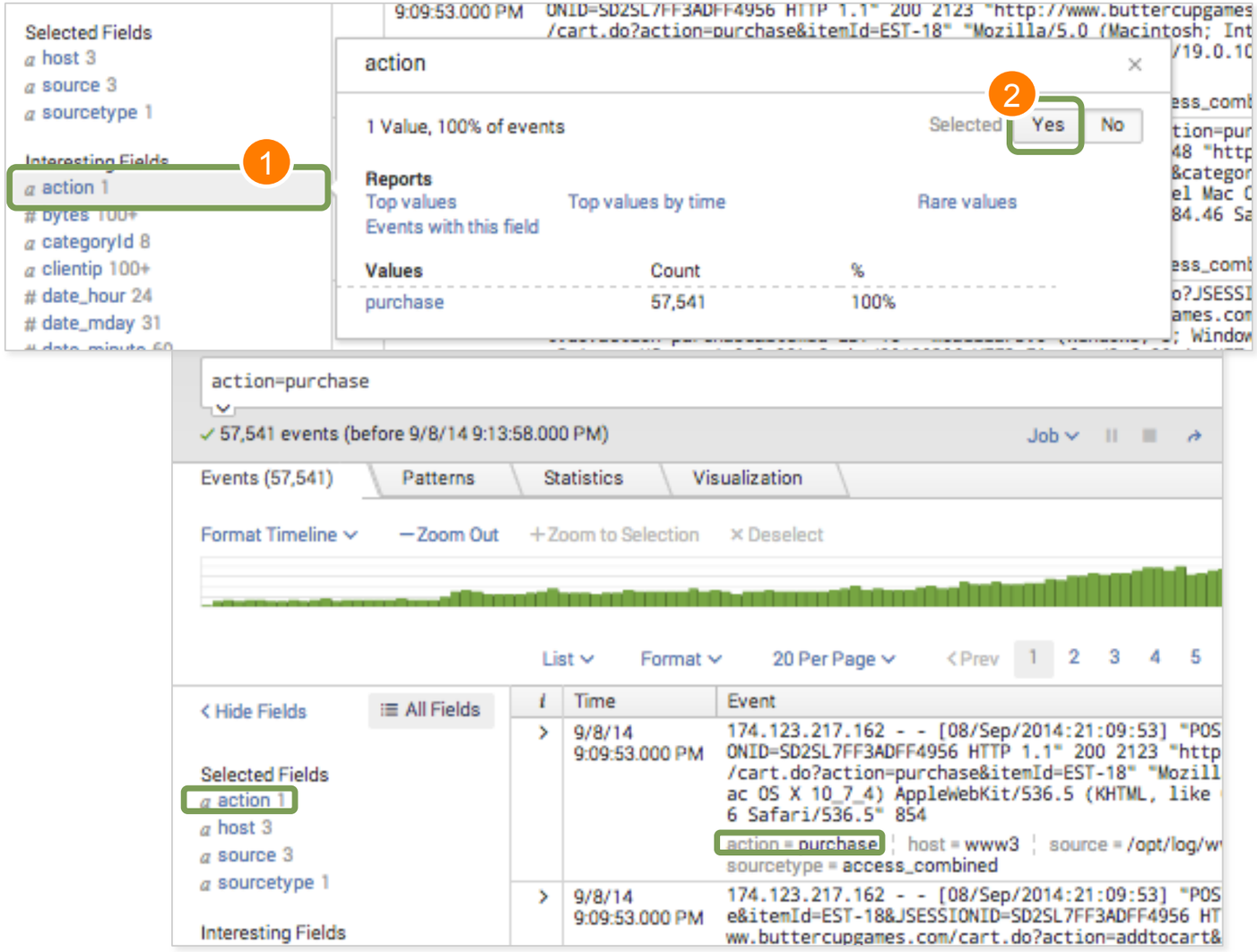
Make an Interesting Field Selected

You can modify selected fields

1. Click a field in the Fields sidebar
2. Click **Yes** in the upper right of the field dialog

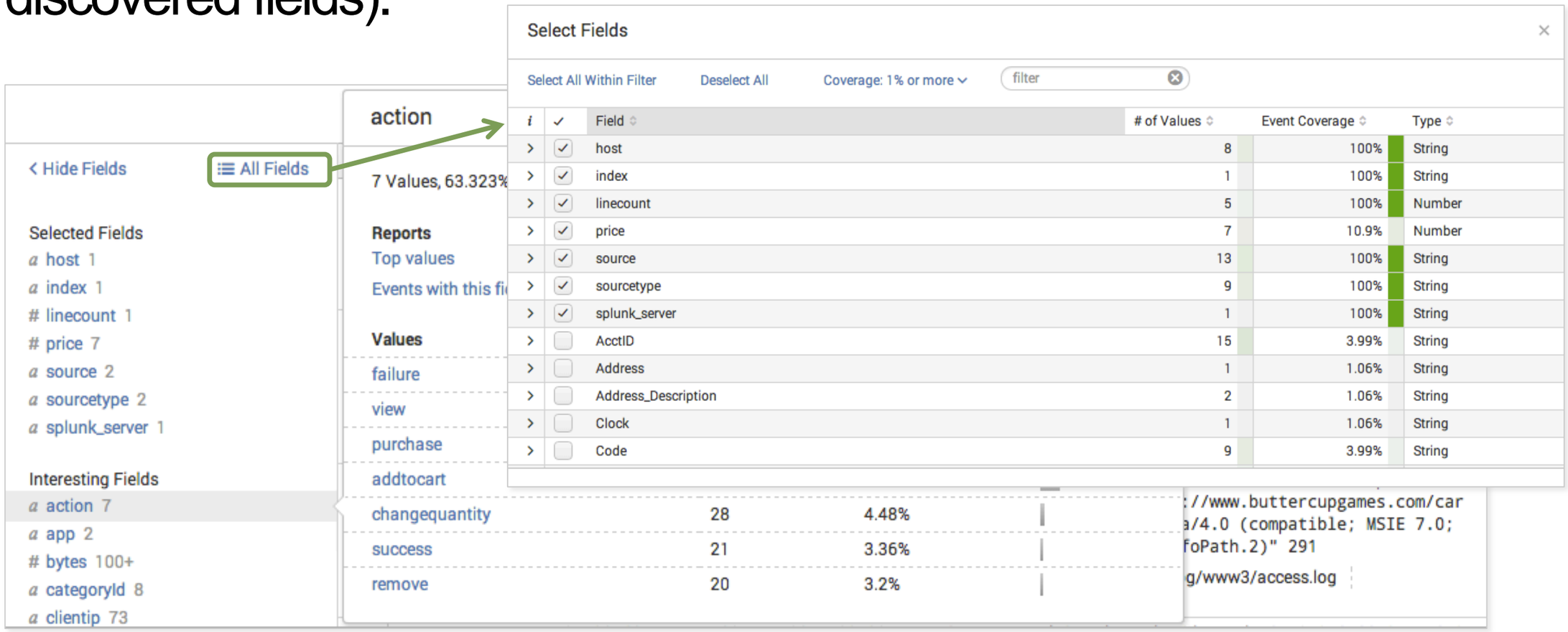
Now that it is a selected field, it appears

- In Selected Fields section of the Fields sidebar
- Below each event where the field exists



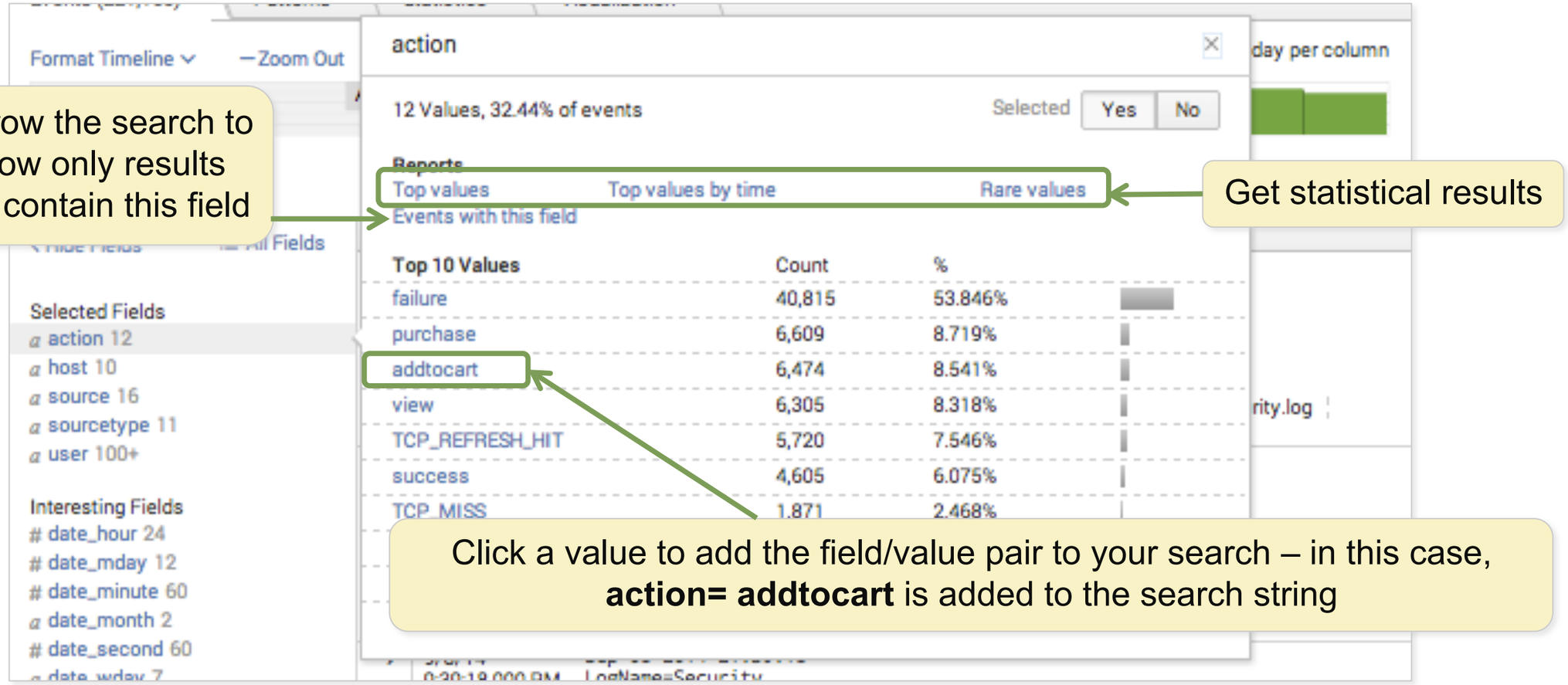
Make Any Field Selected

- You can tag fields as selected fields from All Fields (which shows all of the discovered fields).



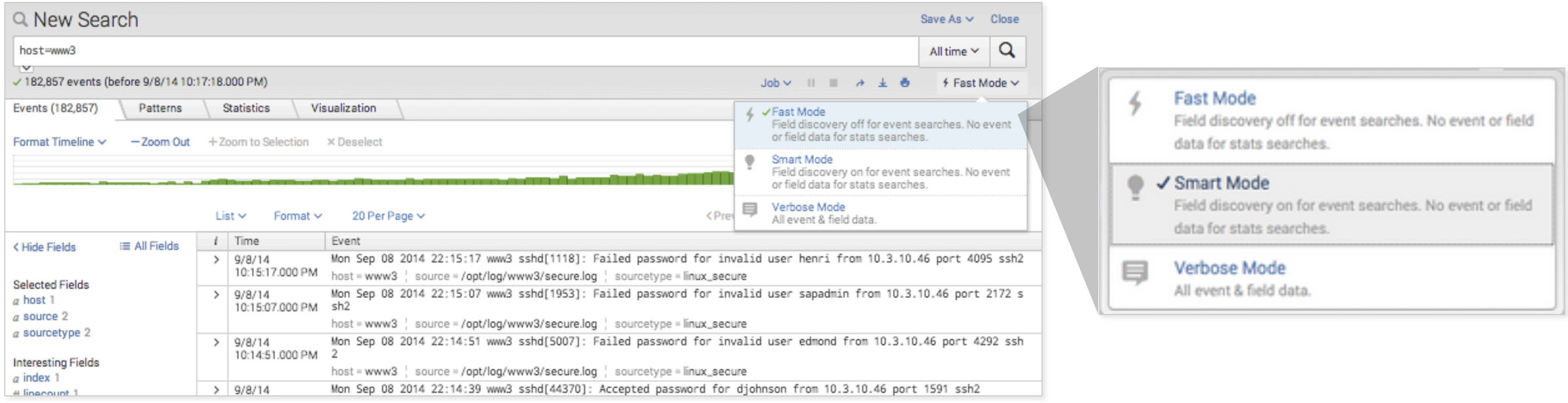
The Field Window

Select a field from the fields sidebar, then:



Search Modes: Fast, Smart, Verbose

- Fast and Verbose modes are the two ends of the search mode spectrum.
  - The default Smart mode switches among them depending on the type of search
  - When you first run a saved search, it will run in the mode in which it was saved
- Based on your needs for each search, select an effective search mode



Quick Overview of Search Modes

Search Mode →	Fast	Smart	Verbose
Emphasizes →	Speed	Balance of speed and completeness	Completeness (but slower)
When run with an event search, • Access to Events view? • Field discovery on? • Fields sidebar exists? • Statistics, Visualization tabs empty?	• Yes • No • Yes • No	• Yes • Yes • Yes • Yes	• Yes • Yes • Yes • Yes
When run with a reporting/statistical search, • Access to Events view? • Field discovery on? • Fields sidebar exists?	No	No	Yes
Default Search Mode?	No	Yes	No

Creating Reports and Visualizations

Module Objectives

- Save a search as a report
- Edit reports
- Create reports that include visualizations such as charts and tables

Reports

- Reports are saved searches
- Reports can show events, tables (statistics), or charts (visualizations) to find trends and help analyze your search results
- Running a report returns fresh results each time you run it
- Statistics and visualizations allow you to drill down by default to see the underlying events
- Reports can be shared and added to dashboards
- You can edit saved reports or create a new report using **Save As**
- There are two ways to create a report: pivot or search

Smart Naming

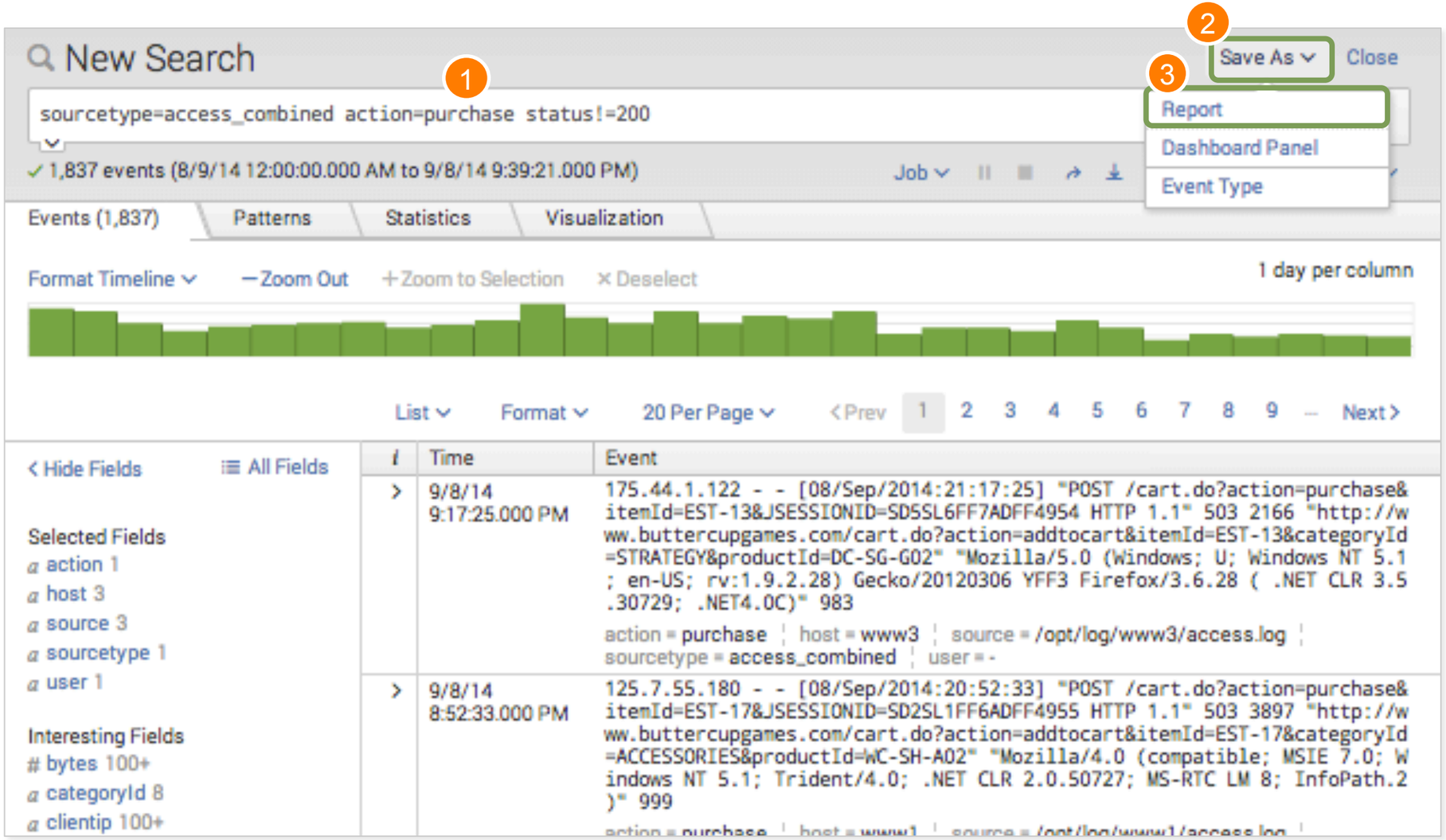
- Before you begin using Splunk on the job, define a naming convention so you can always find your reports, and tell them all apart.
  - For example you can create something simple like this:
    - <group>_<object type>_<object description>
      - Group: the name of the group or department using the knowledge object such as sales, IT, finance, etc.
      - Object type: report, dashboard, macro, etc.
      - Object description: Weekly sales, failed logins, etc.
  - A weekly sales report can be identified as:
    - sales_report weekly_sales
- This course uses simple names so you can focus on key learning points.

Note

If you set up naming conventions early in your implementation, you can avoid some of the thornier object naming issues. The example is a suggestion. The details are found in our docs: http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Developnamingconventionsforknowledgeobjecttitles

Create a Report from Search

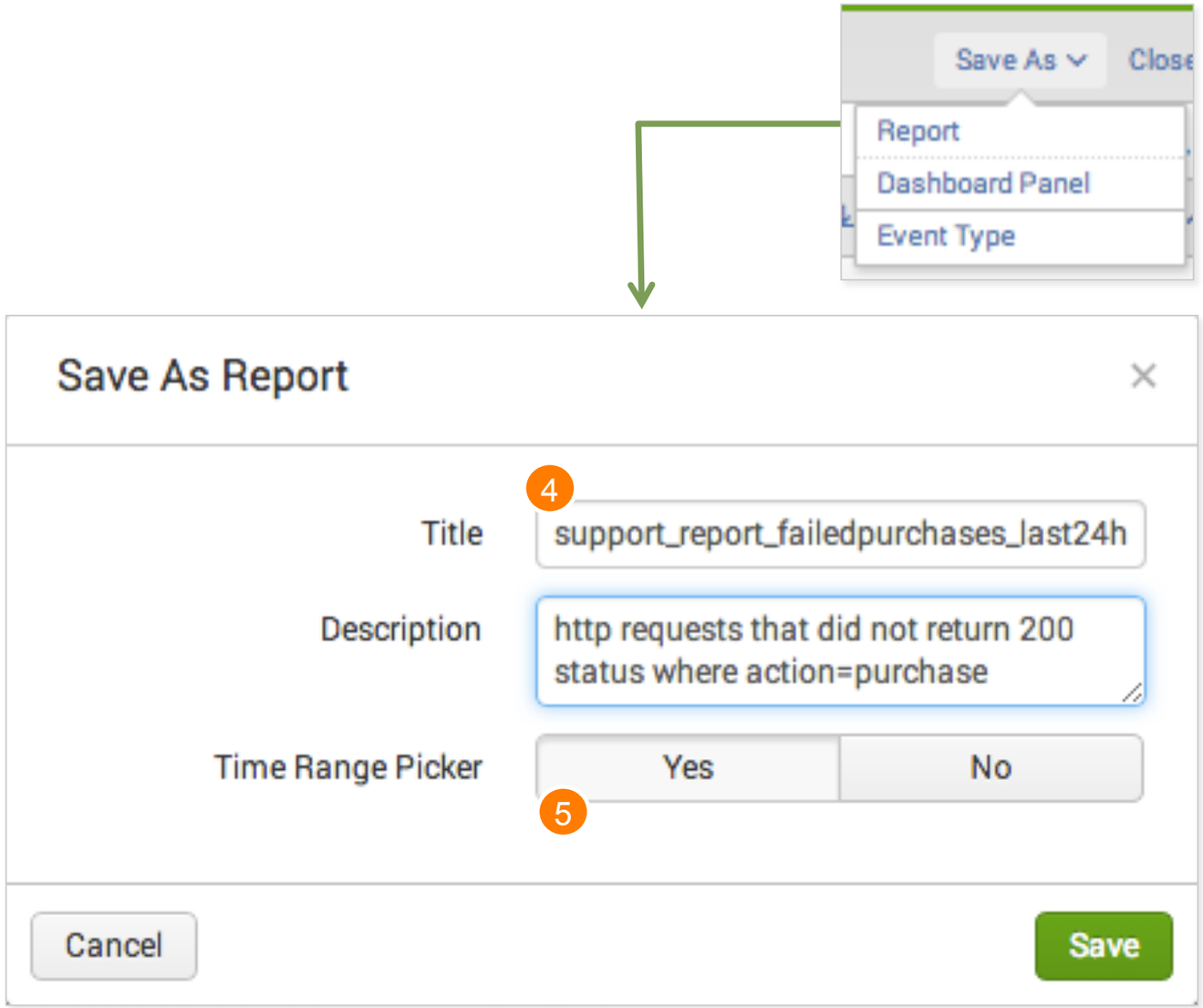
1. Run a search
2. Select **Save As**
3. Select **Report**



Create a Report from Search (cont.)

4. Give the report a meaningful title and description (optional)
5. Select whether to include or not to include a time range picker

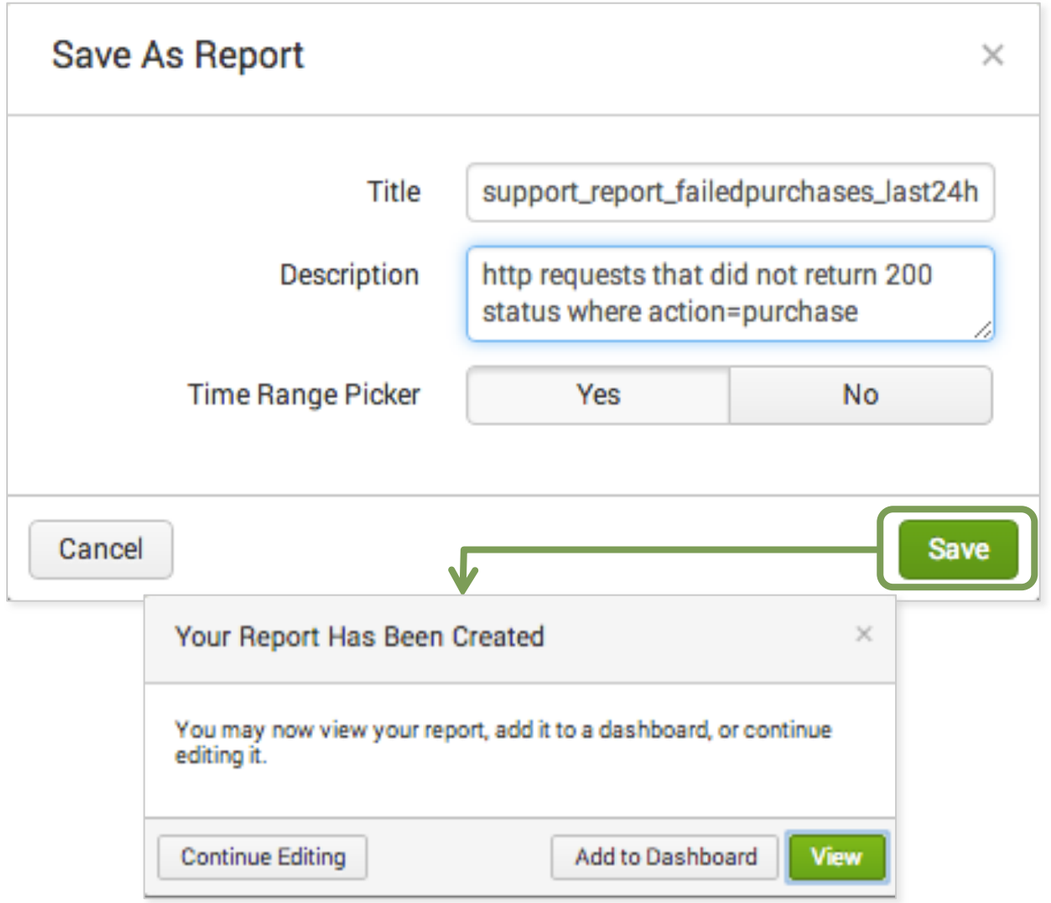
Adding a time range picker allows you to adjust the time range of the report when you run it



Create a Report from Search (cont.)

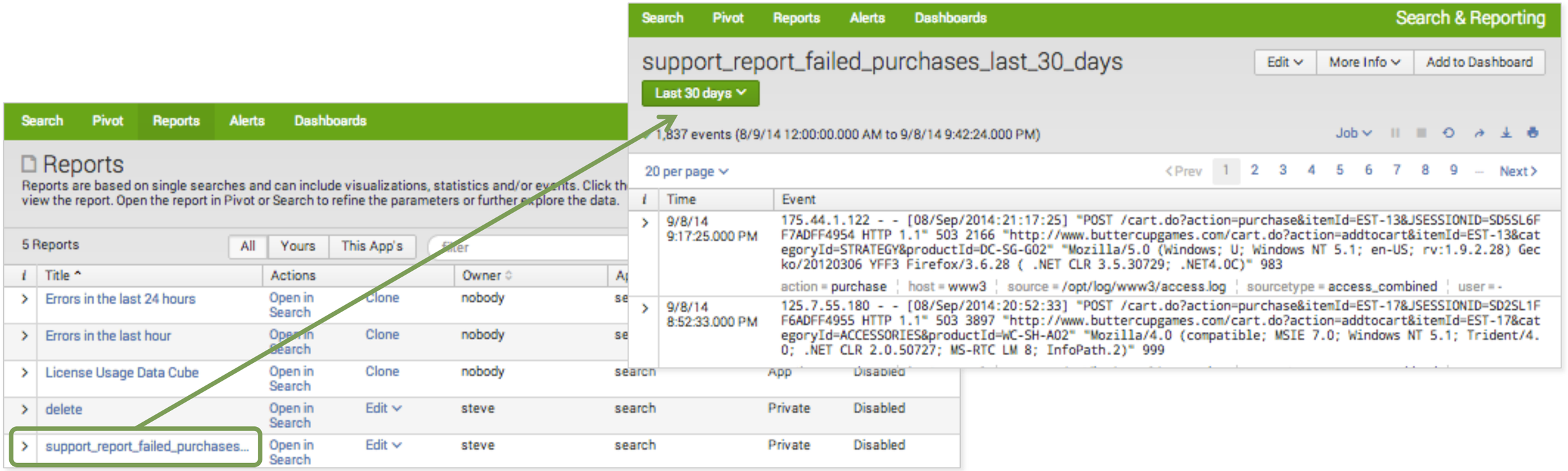
You can change Additional Settings:

- Click **Continue Editing** to make changes to your report
- Click **Add to Dashboard** to add your report to a dashboard
- Click **View** in the lower right to see your report or run it again



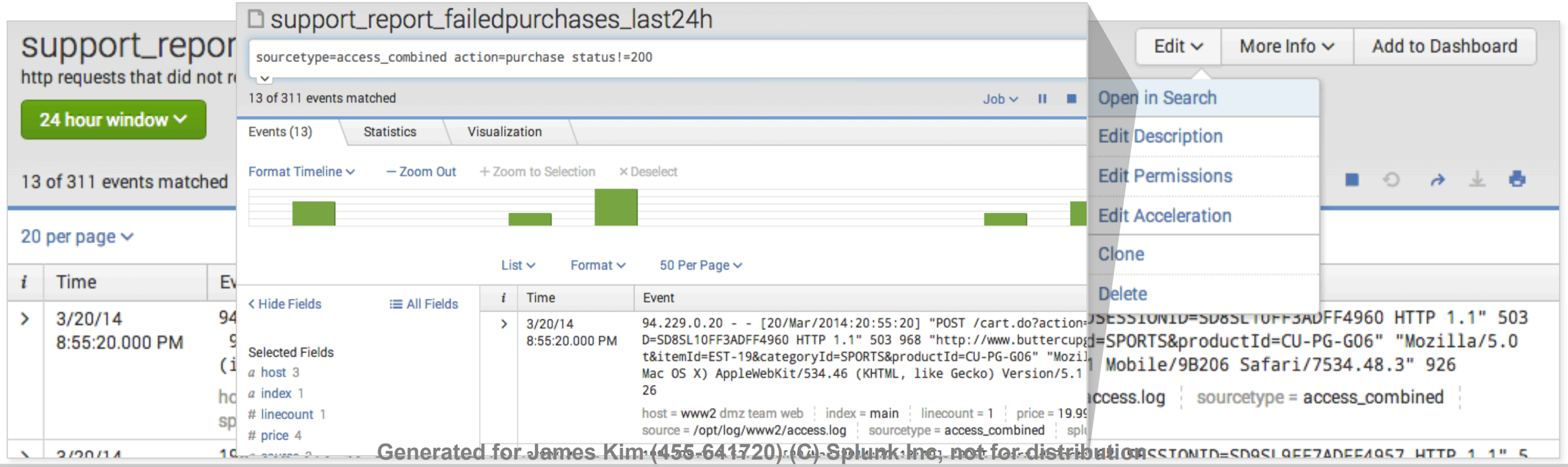
Running Reports

- Click **Reports**, then click the report title to run it. The report runs using the time range that was specified when it was saved.
- Use the time range picker to change the time range of the report (if available)



Edit Reports

- To edit a report's underlying search, select **Edit > Open in Search**
  - You can then edit and re-save, not save, or save-as a new report
- You can also edit the description, permissions, schedule, and acceleration, or you can clone or delete the report



Create Tables and Visualizations

Three main methods to create visualizations in Splunk:

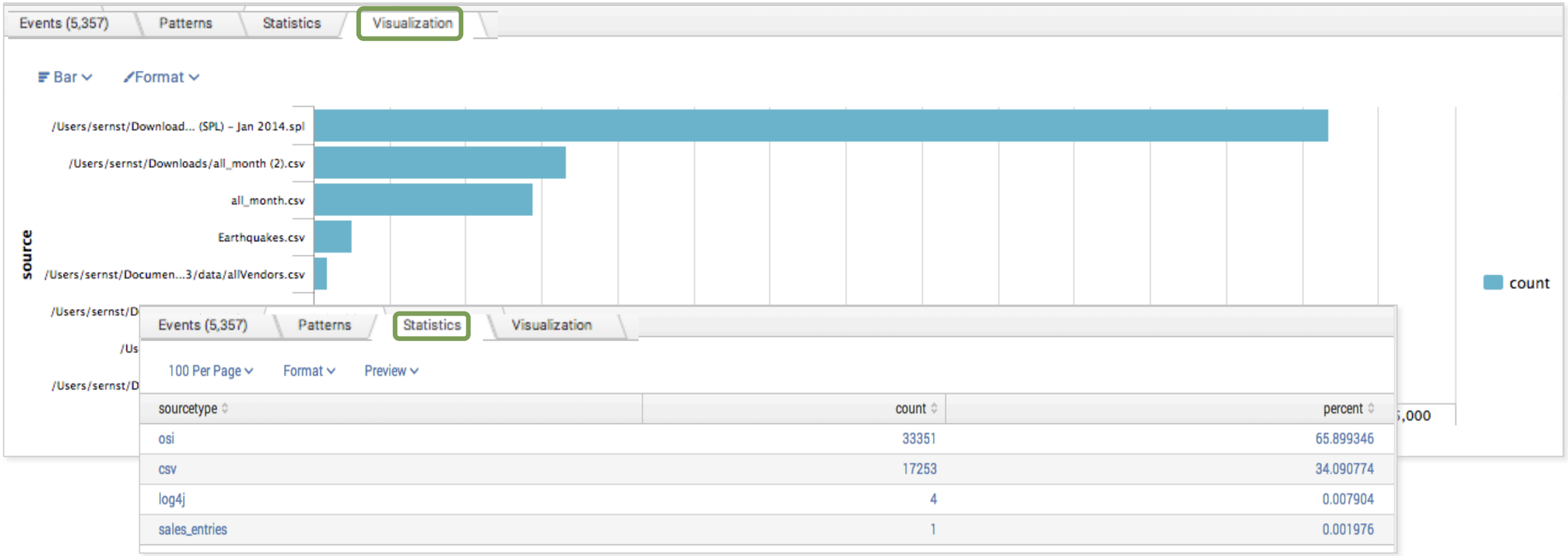
- Select a field from the fields sidebar
- Use the Pivot interface
  - Start with a data model

  or

  - Start with Instant Pivot
- Use the Splunk search language commands in the Search bar with Statistics and Visualization tabs

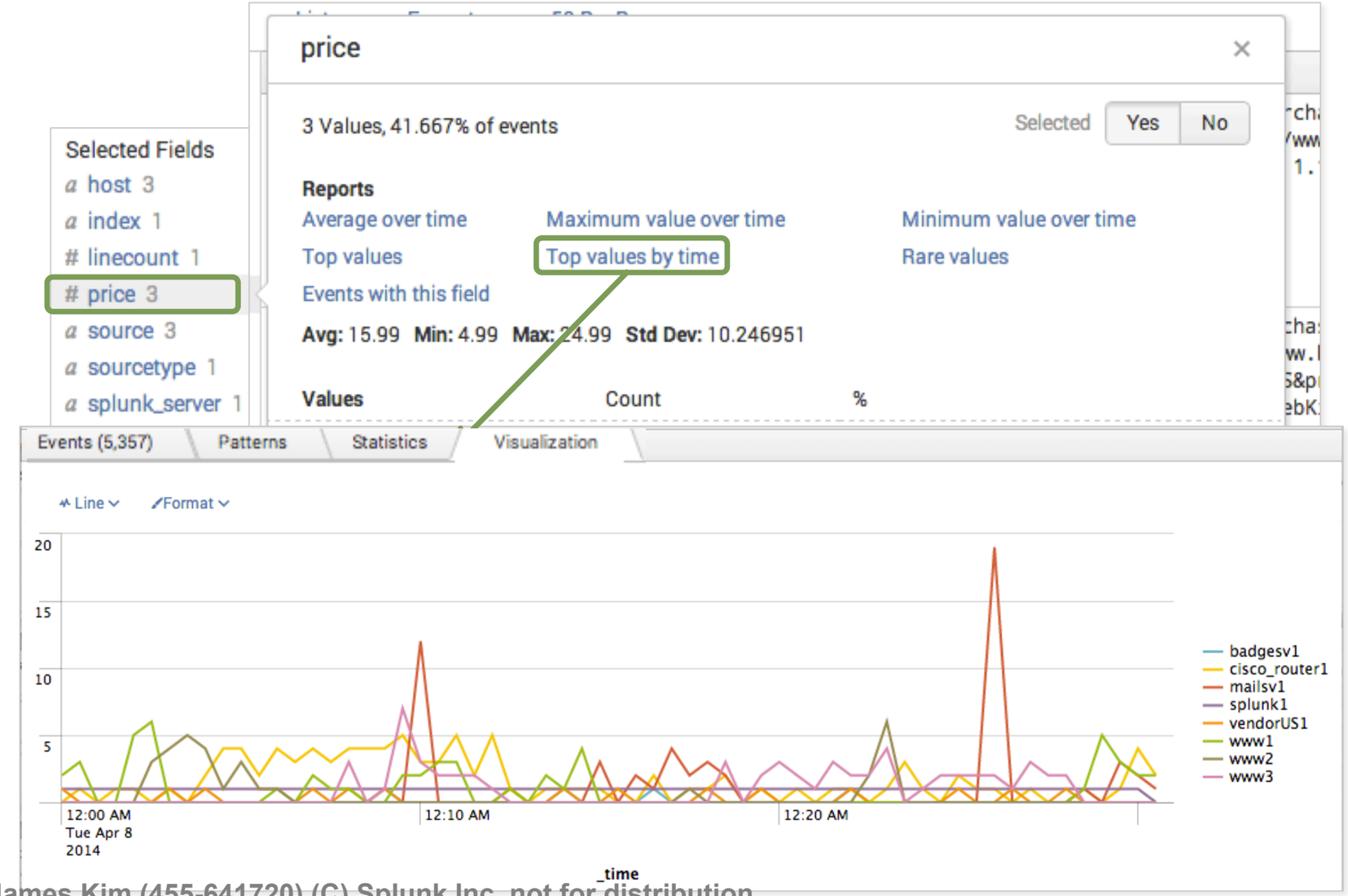
Tables and Visualizations

- Statistical reports leverage Splunk's built-in visualizations or table format
- These views give you insights into your organization's data



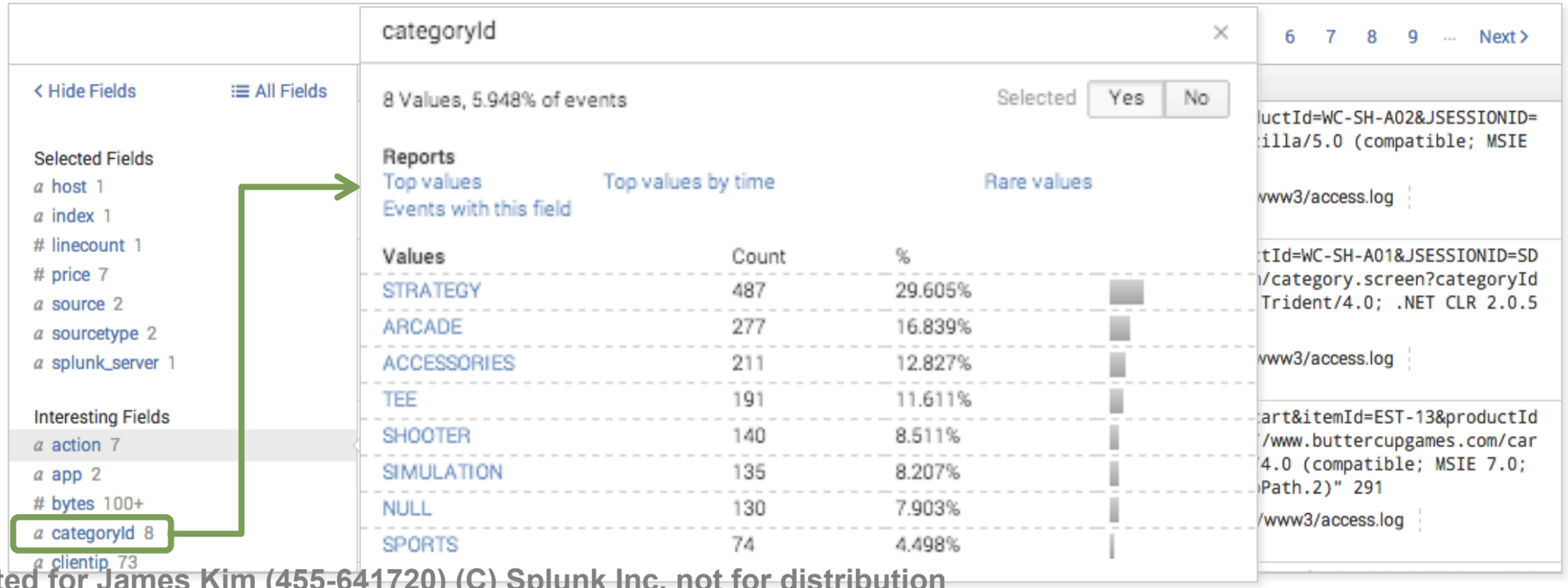
Create Reports From the Field Window

- For numeric fields, you can create reports with mathematical functions such as average, maximum value, and minimum value
- In this example, it generates a report that shows top values by time
  - This is known as a timechart



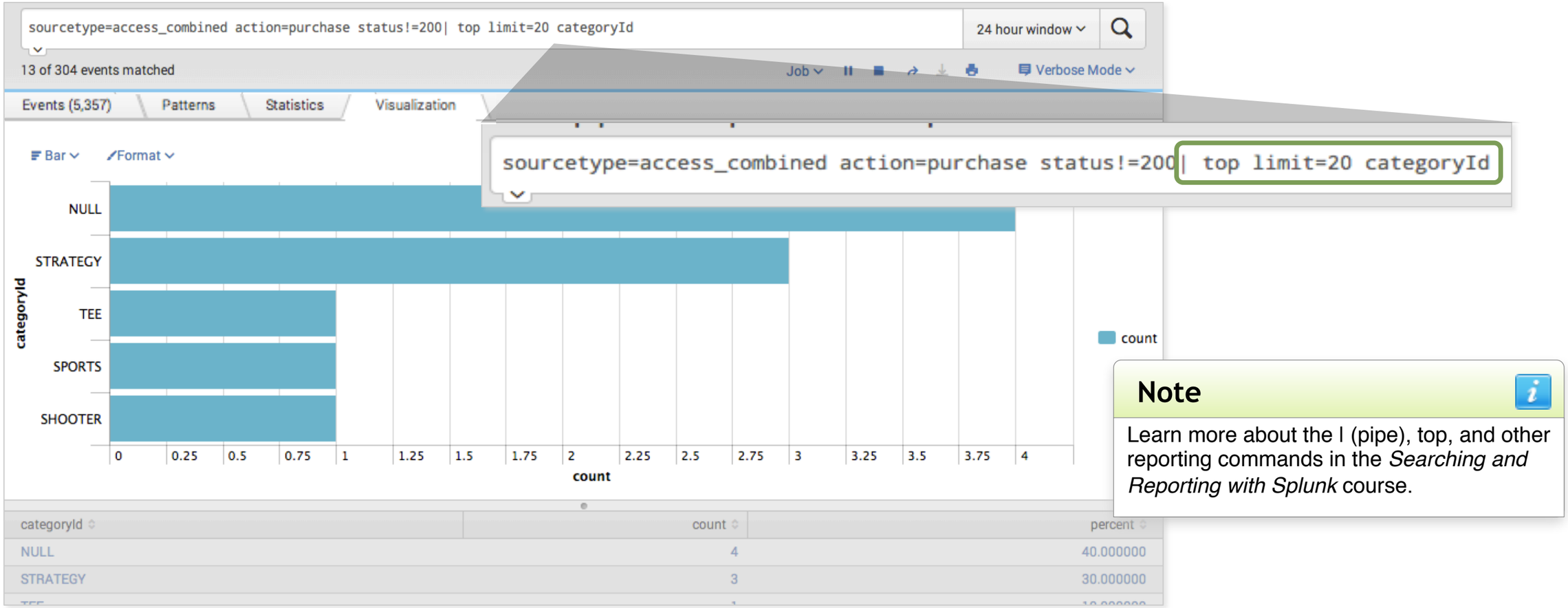
Create a Top Values Report

- For character fields, there are only 3 available reports
- We want a report that show us the top **categories** purchased
  - Example search: `sourcetype=access_combined status=200 action=purchase`
  - Click the **categoryId** field
  - Click **Top values**



Create a Top Values Report (cont.)

A | (pipe) and the top command is added to the search string and returns a bar chart on the Visualizations tab of the top categories purchased

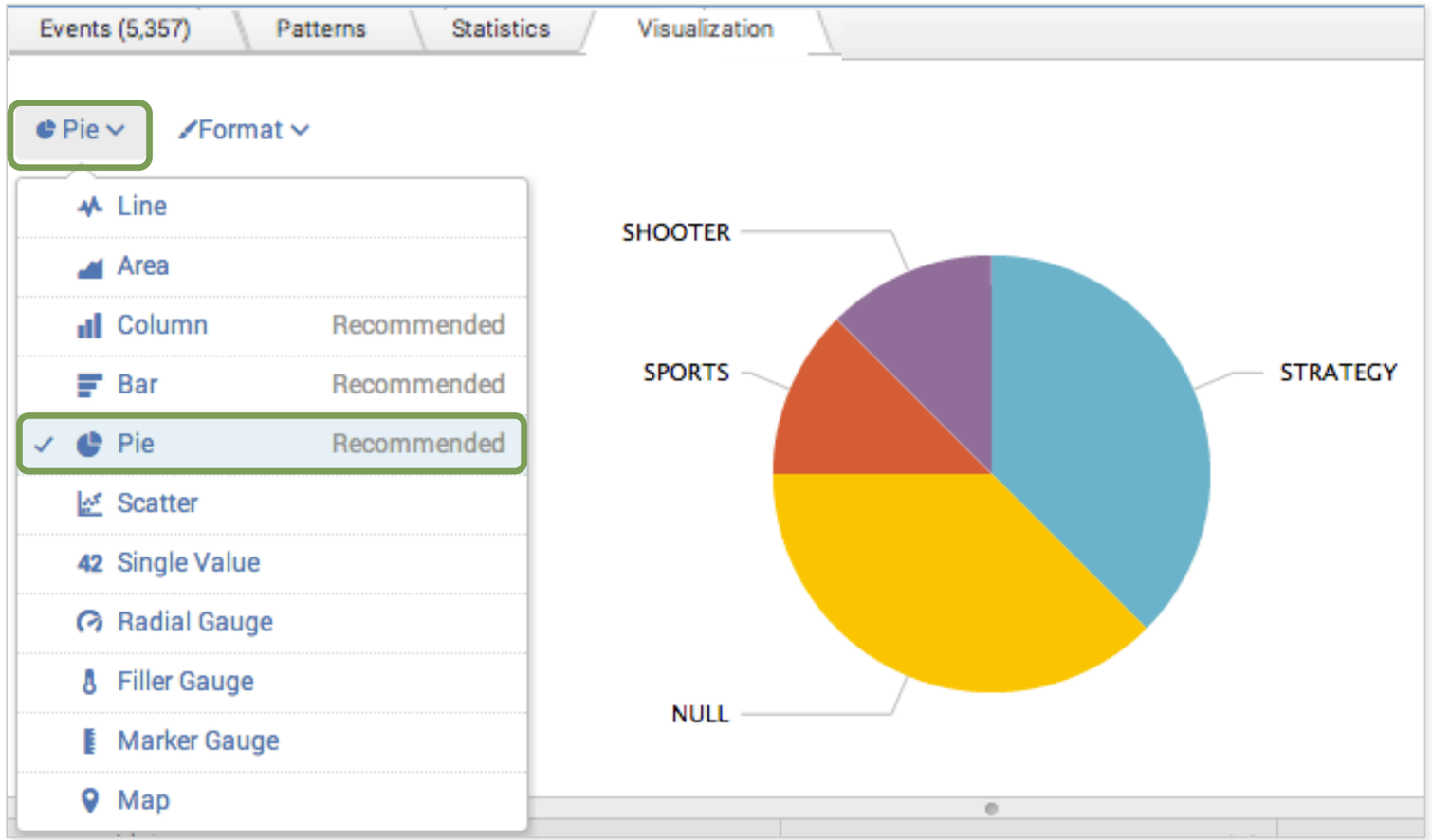


Note

Learn more about the | (pipe), top, and other reporting commands in the *Searching and Reporting with Splunk* course.

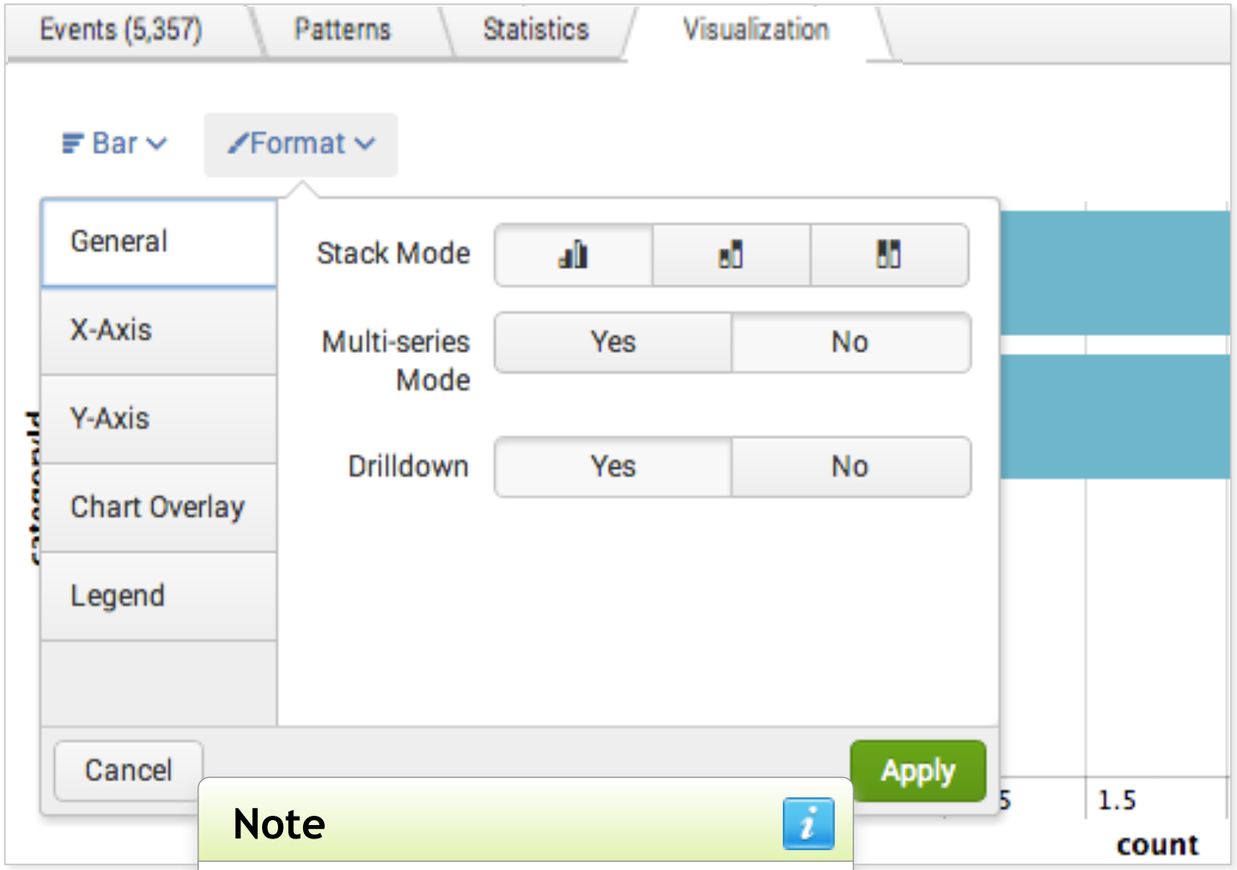
Change the Visualization

- Select a visualization from the **Type** dropdown menu
- In this example, the bar chart is changed to a pie chart



Change the Format

- The **Format** menu allows you to change formatting options for certain types of visualizations
- For bar and column charts, you can change the **stack** and **multi-series** modes, **axis** labels, and **legend**
- The **Drilldown** option determines whether or not clicking on the chart drills down on a specific value in the search and returns events

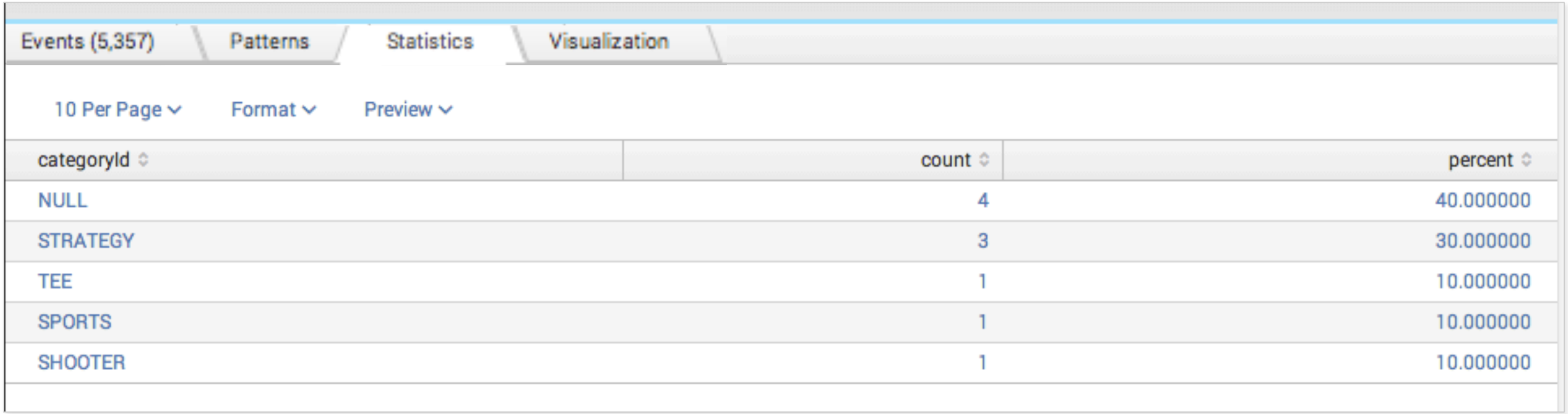


Note

Learn more about modes and axes in the Searching *and Reporting* class. These modes require more sophisticated searches.

View as a Table

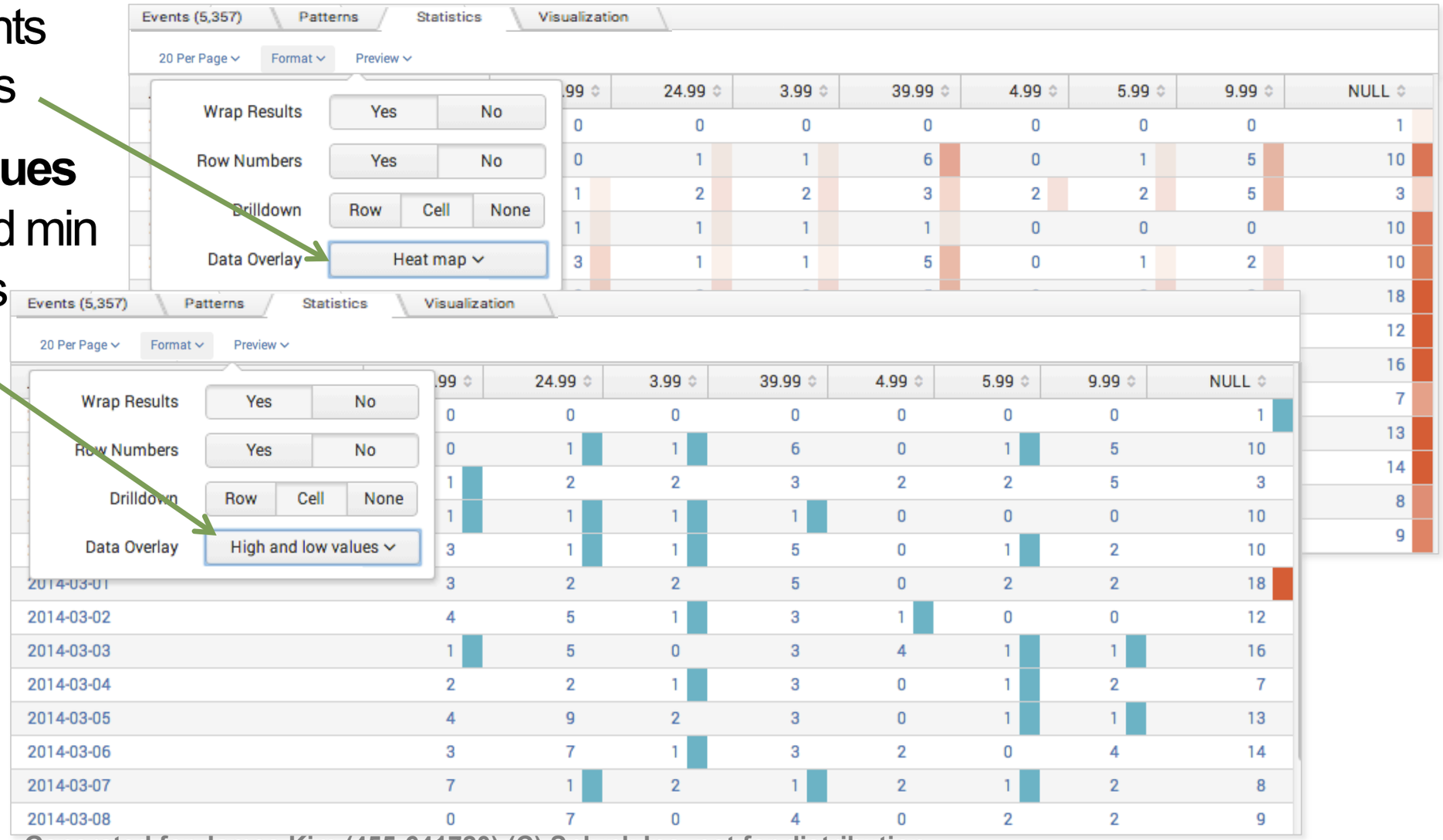
Switch to the **Statistics** tab to view the results as a table



categoryId	count	percent
NULL	4	40.000000
STRATEGY	3	30.000000
TEE	1	10.000000
SPORTS	1	10.000000
SHOOTER	1	10.000000

Statistics Overlays

- **Heat map** highlights outstanding values
- **High and low values** highlights max and min of non zero values



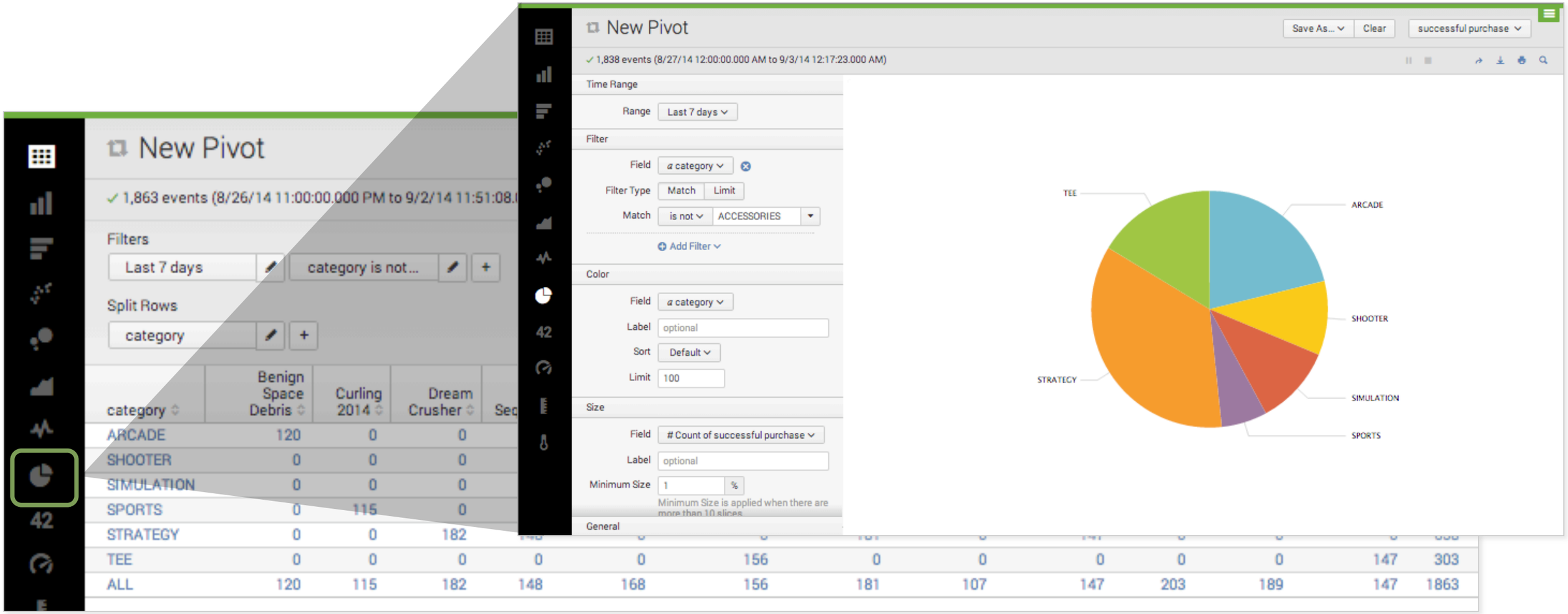
Using Pivot

Objectives

- Describe pivot
- Understand the relationship between the data model and the pivot
- Select a data model object
- Create a pivot report
- Use instant pivot to create a report

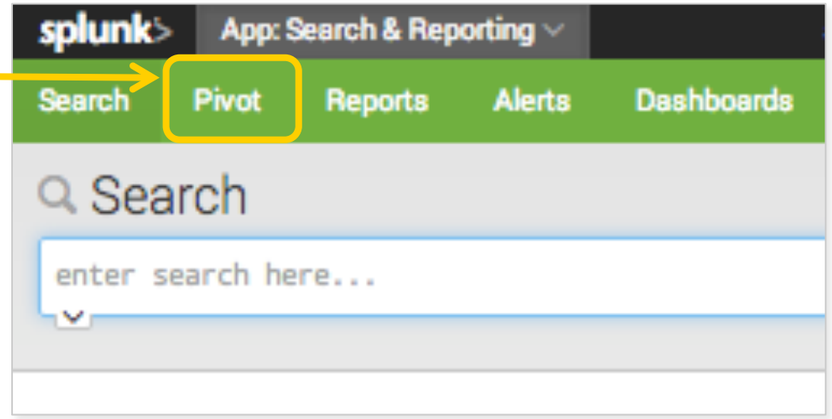
Completed Pivot

Pivot is a quick way to design visualizations of data. Let's see how.



Select a Data Model

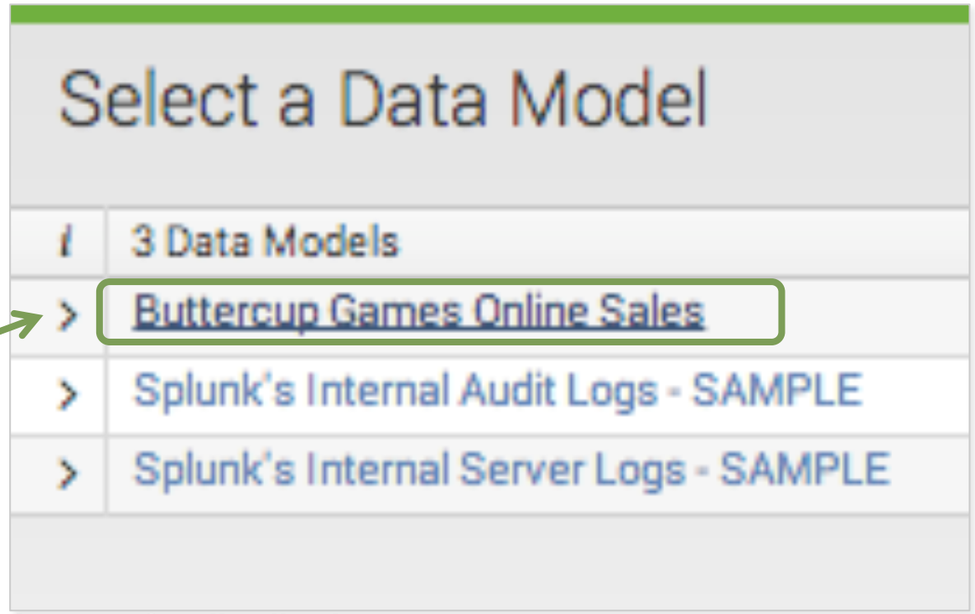
1. From the Search & Reporting app, select the **Pivot** tab to display a list of available data models
   - Each data model represents a specific category of data



Note

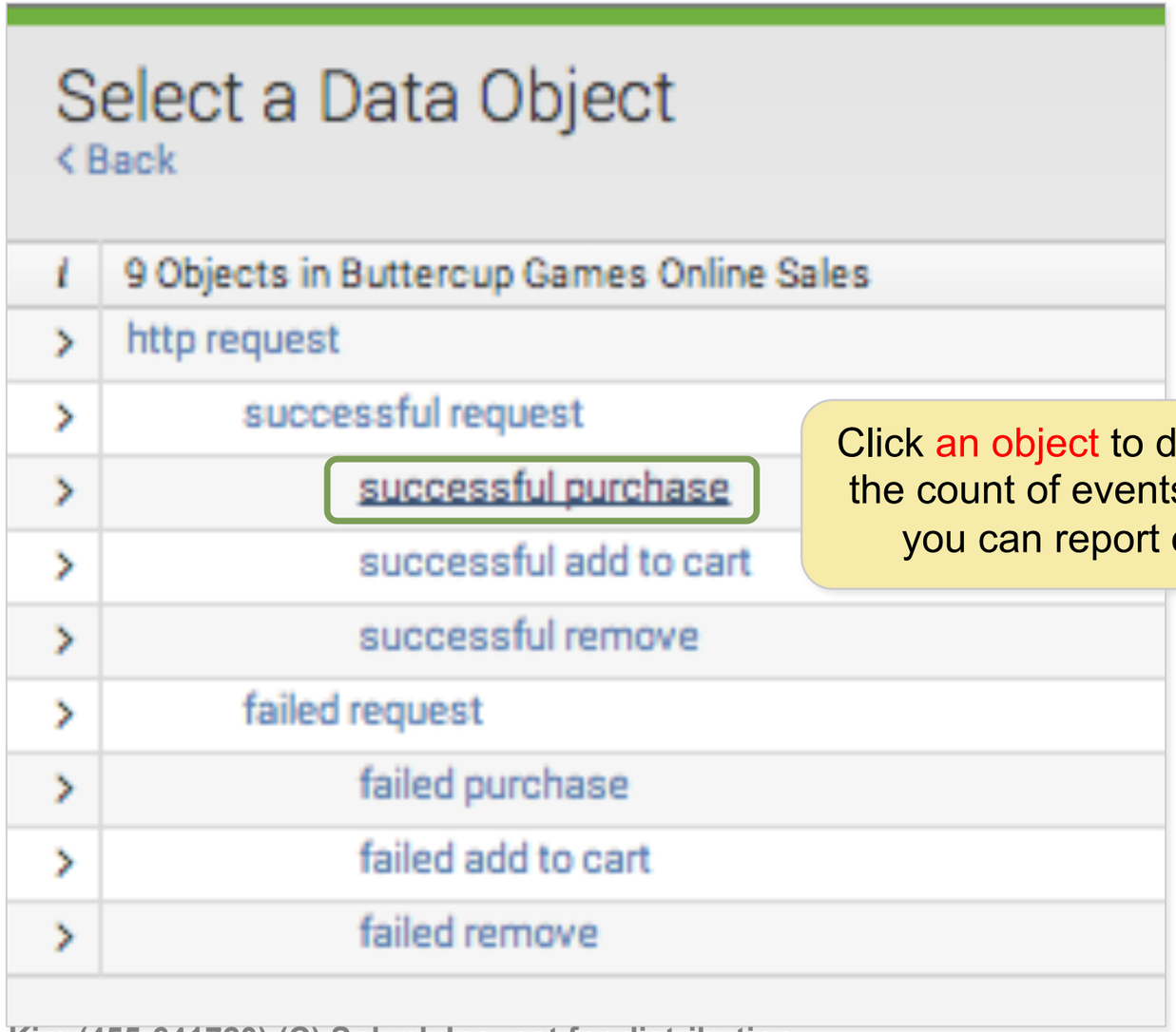
Learn to build data models (which are foundational to pivots) in the *Creating Splunk Knowledge Objects* course.

2. Select Buttercup Games Online Sales
   - This data model is based on online sales activity



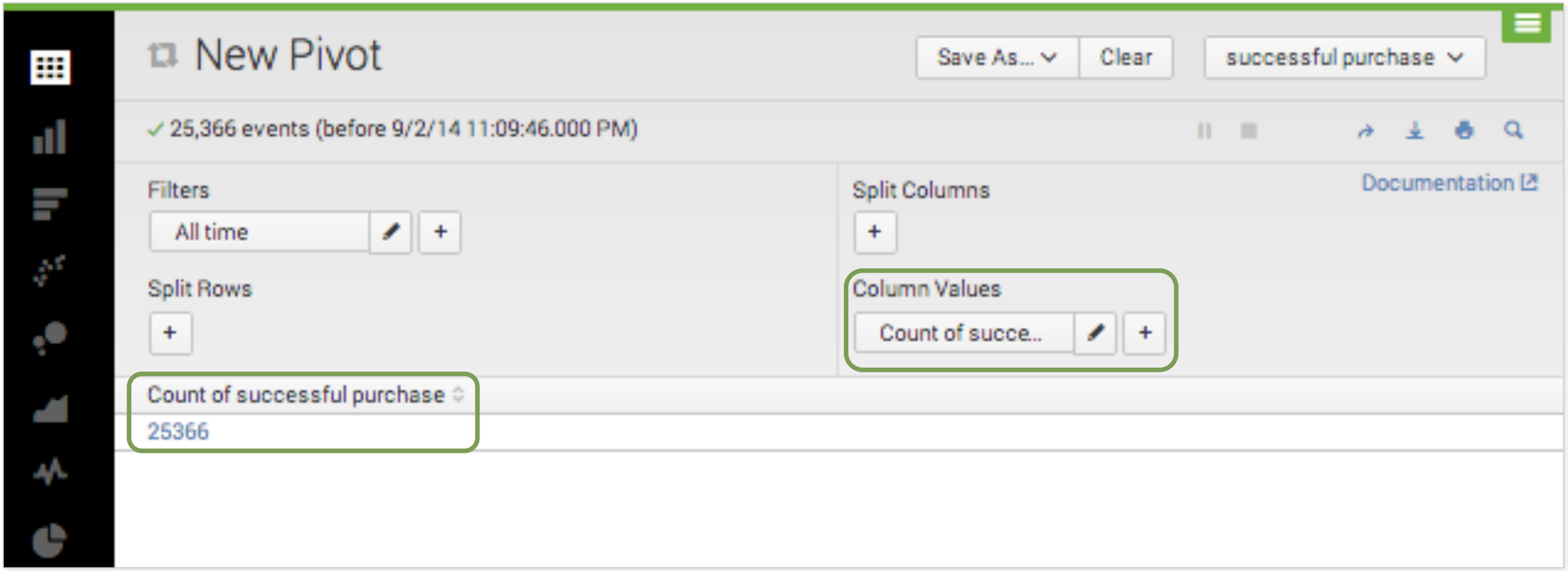
Select an Object

- After you select a data model, a list of objects appears
- Each object represents a specific set of events, in a hierarchical structure
- Example: select the **successful purchase** object



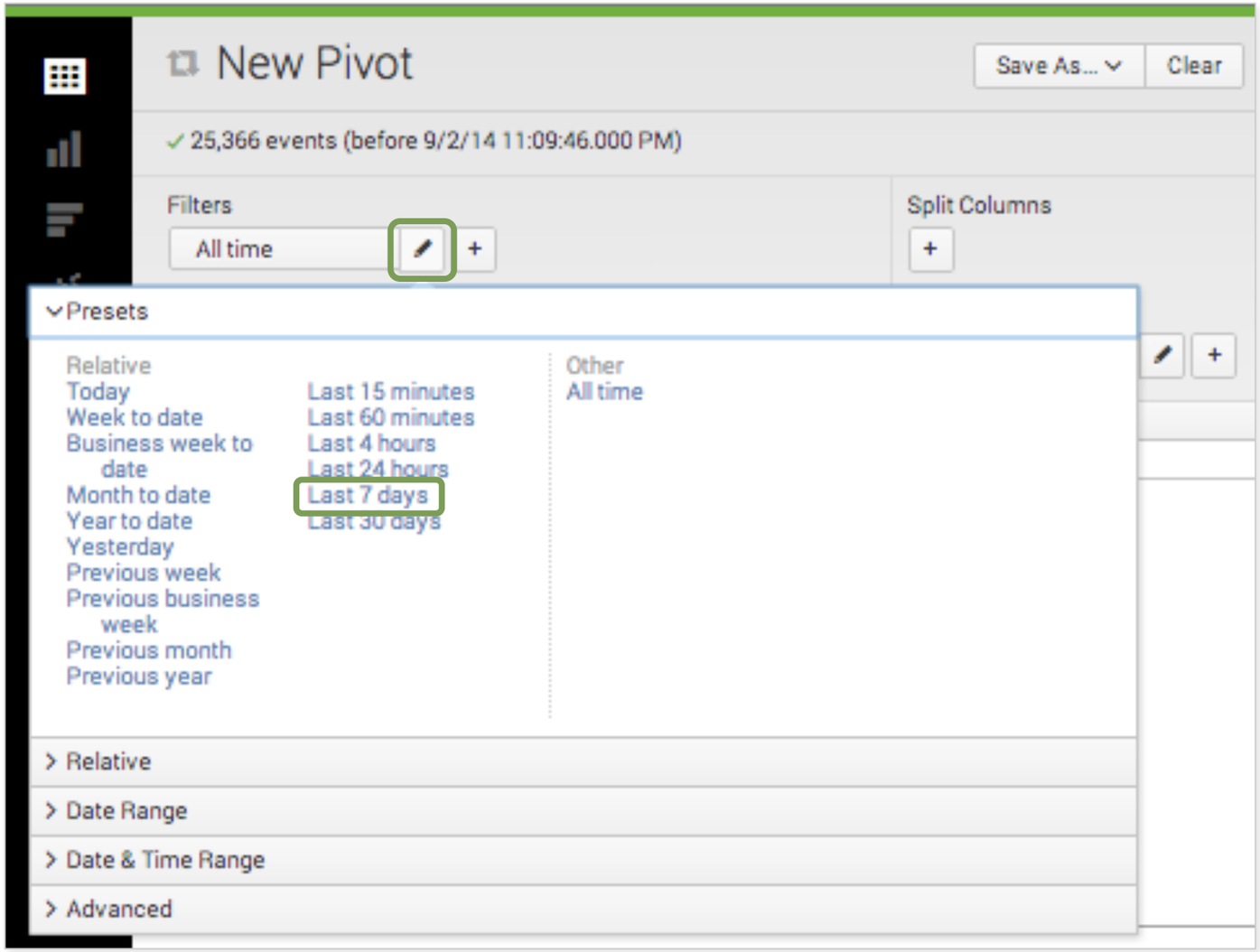
Open in Pivot

The Pivot automatically populates with a count of events for the selected object; in this example, all successful purchase requests for all time



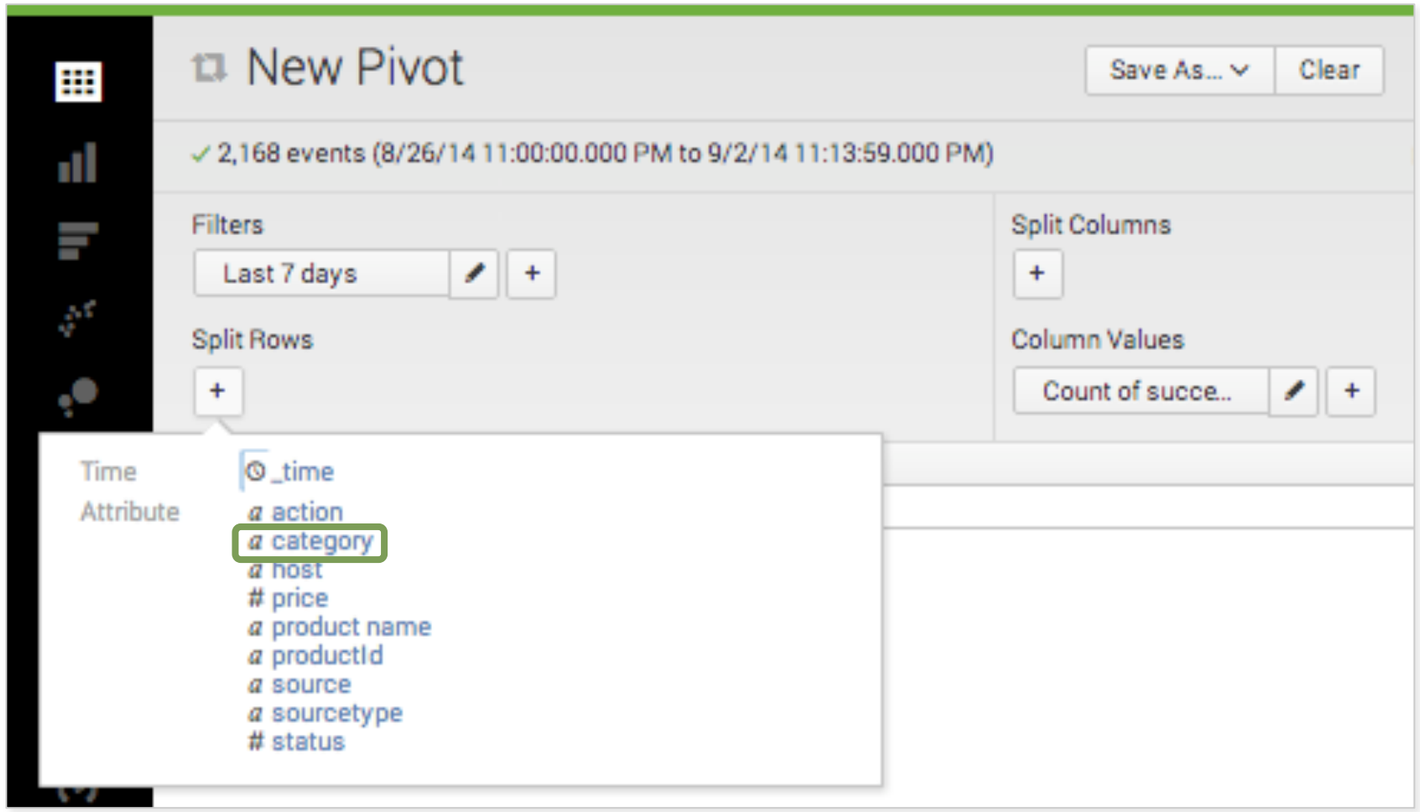
Select a Time Range

- The default is **All Time**
- Click the pencil icon to select the desired time range
- The pivot runs immediately upon selecting the new time range



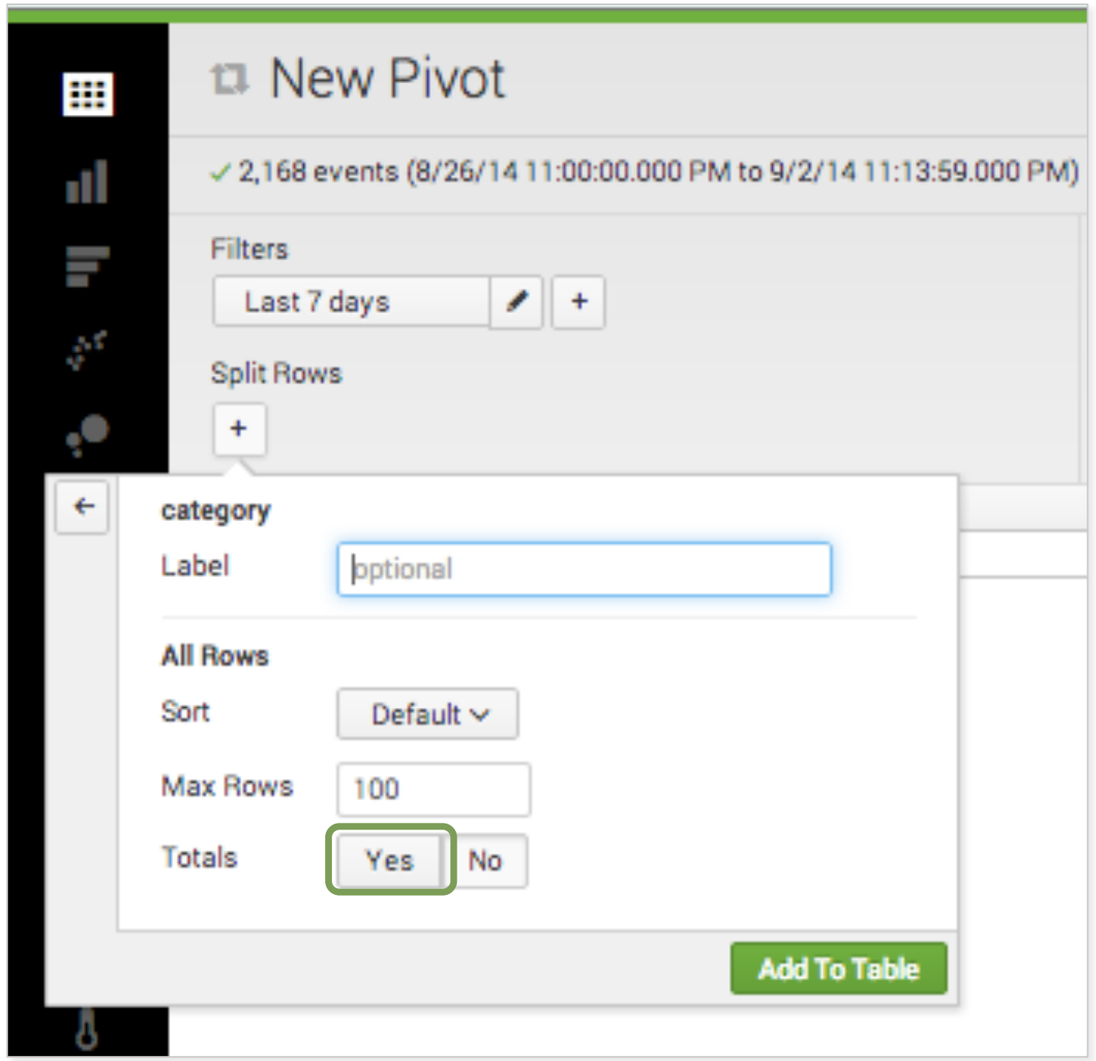
Split Rows

- Click + under **Split Rows** for a list of available fields to populate the rows
- In this example, we'll split the rows by **category**
  - This selection gives us a count of successful requests, split by game category

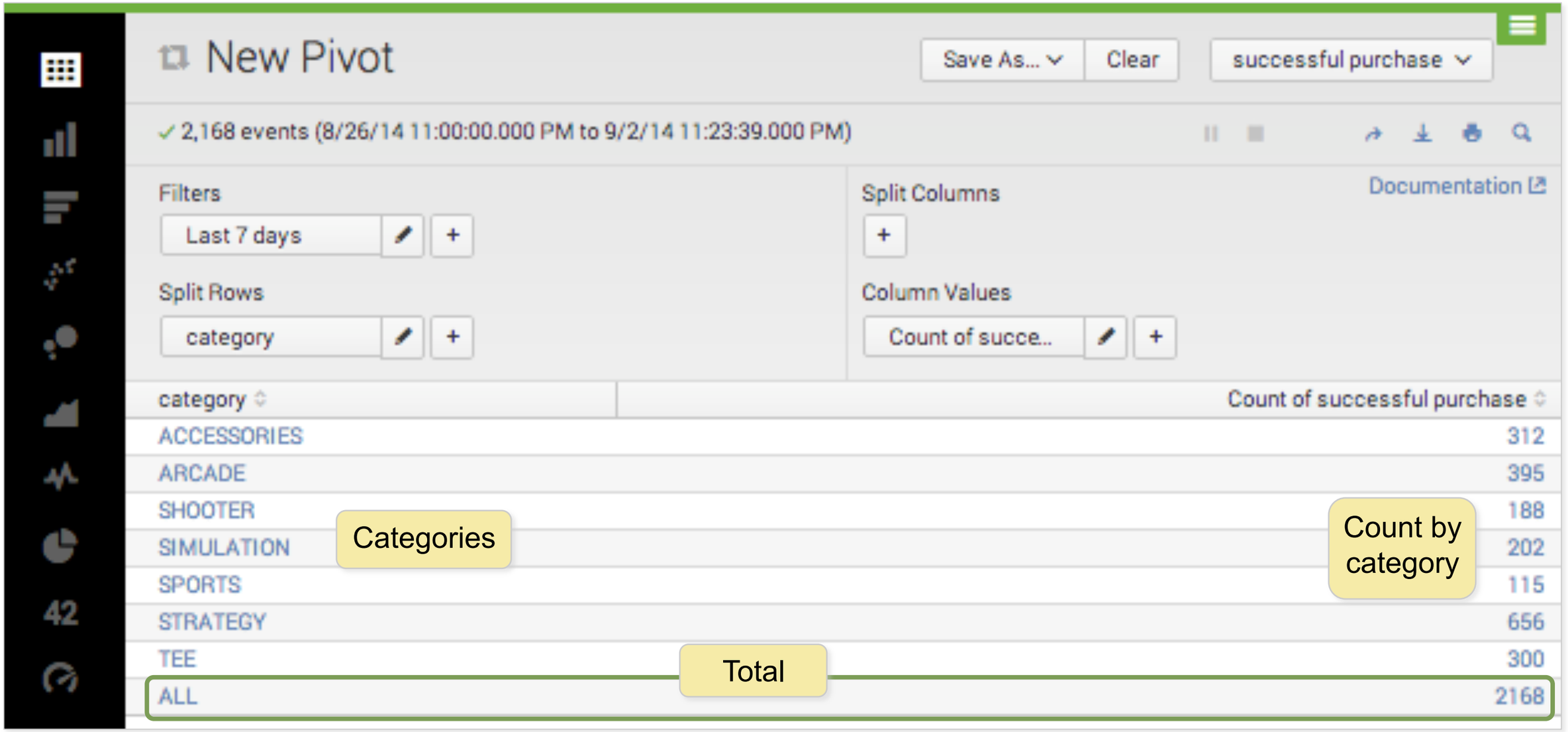


Split Rows (cont.)

- Once selected, you can:
  - Modify the label
  - Change the sort order
    - **Default** – sorts by the field value in ascending order
    - **Ascending** - sorts by the count in ascending order
    - **Descending** – sorts by the count in descending order
  - Define maximum # of rows to display
  - Add **Totals** to your report
- Click **Add to Table** to view the results

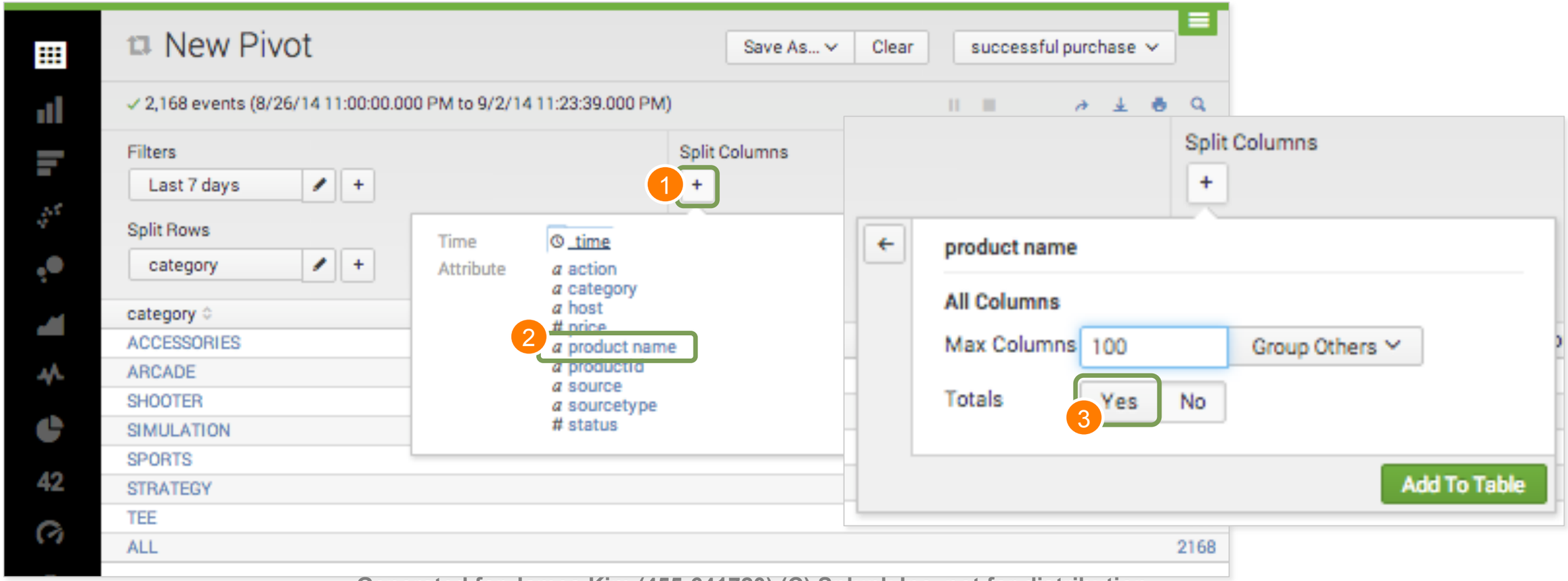


Results

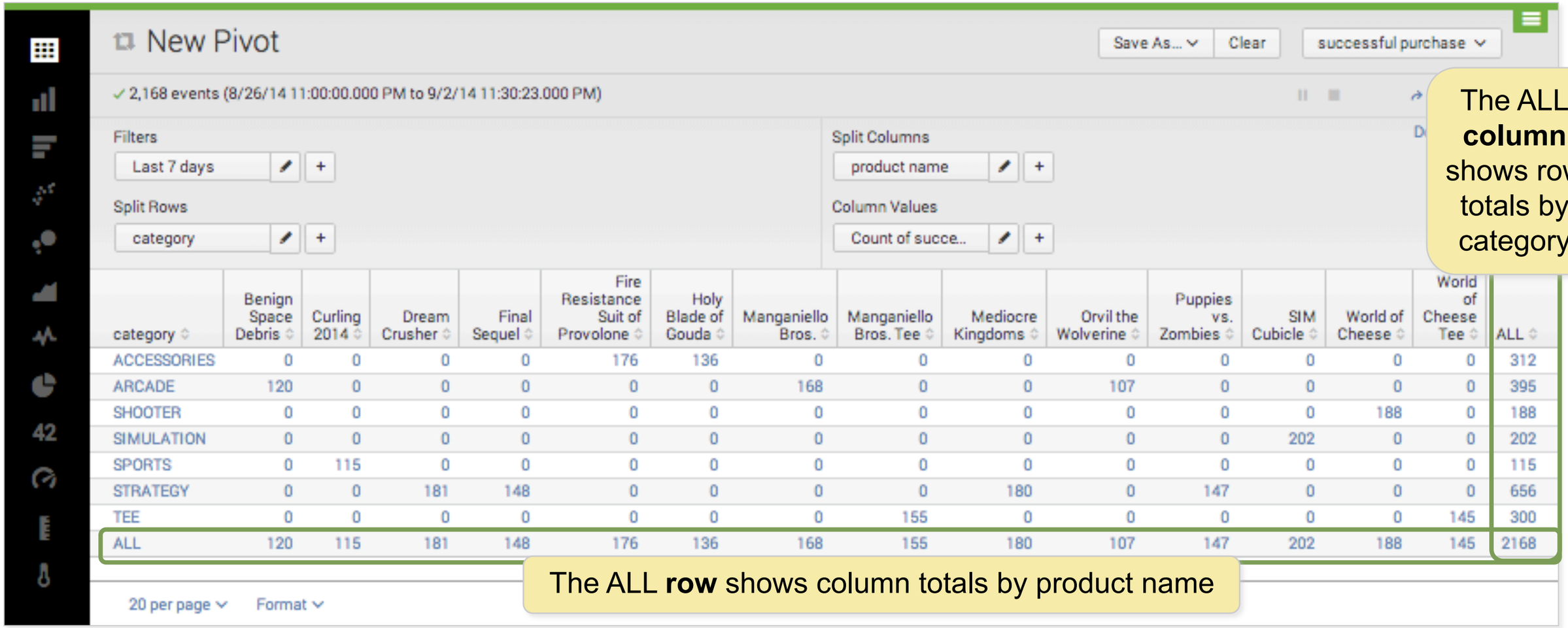


Split Columns

- Click + under **Split Columns** and select the desired split
- Specify the maximum number of columns and whether you want Totals



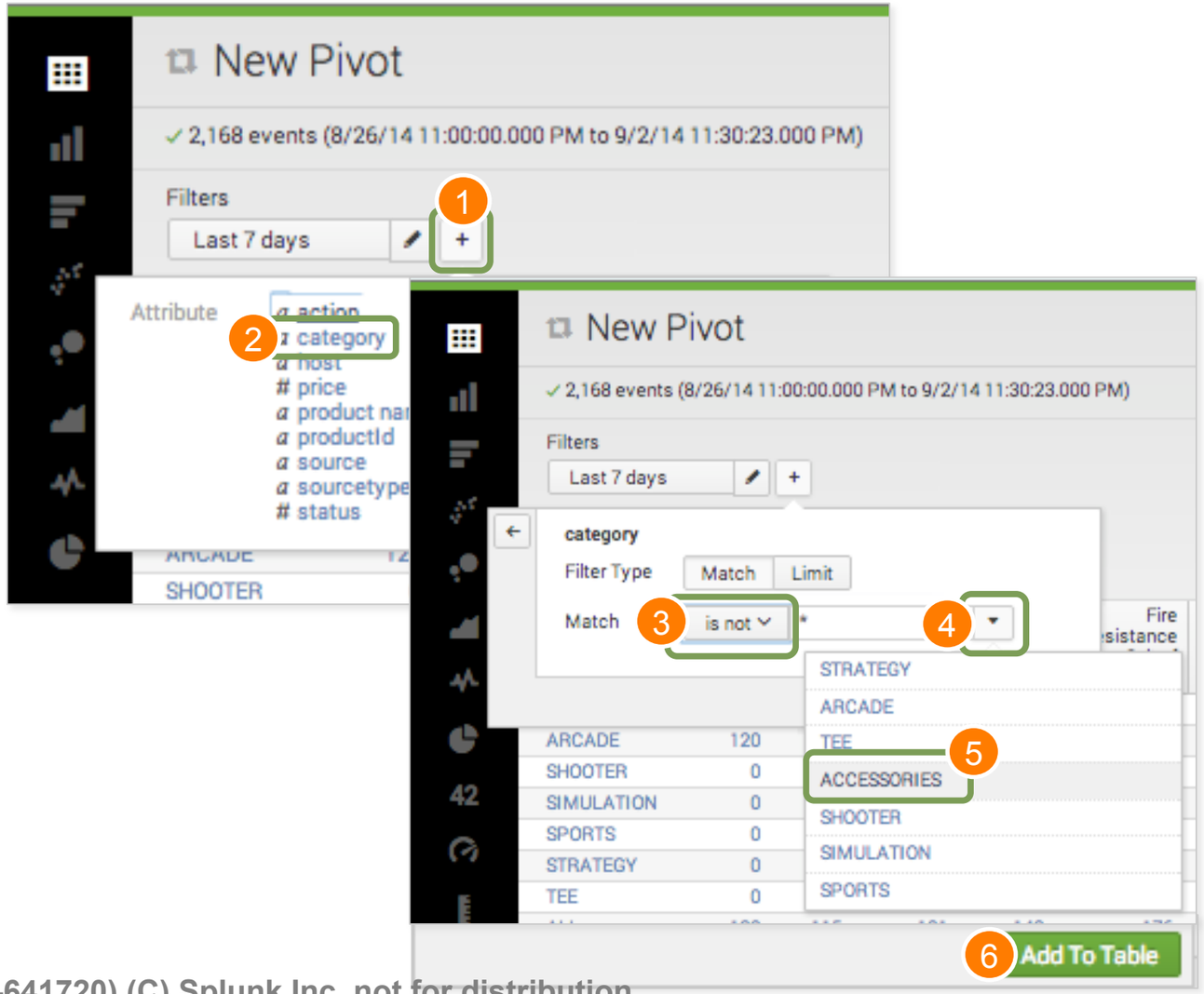
Results



category	Benign Space Debris	Curling 2014	Dream Crusher	Final Sequel	Fire Resistance Suit of Provolone	Holy Blade of Gouda	Manganiello Bros.	Manganiello Bros. Tee	Mediocre Kingdoms	Orvil the Wolverine	Puppies vs. Zombies	SIM Cubicle	World of Cheese	World of Cheese Tee	ALL
ACCESSORIES	0	0	0	0	176	136	0	0	0	0	0	0	0	0	312
ARCADE	120	0	0	0	0	0	168	0	0	107	0	0	0	0	395
SHOOTER	0	0	0	0	0	0	0	0	0	0	0	0	188	0	188
SIMULATION	0	0	0	0	0	0	0	0	0	0	0	202	0	0	202
SPORTS	0	115	0	0	0	0	0	0	0	0	0	0	0	0	115
STRATEGY	0	0	181	148	0	0	0	0	180	0	147	0	0	0	656
TEE	0	0	0	0	0	0	0	155	0	0	0	0	0	145	300
ALL	120	115	181	148	176	136	168	155	180	107	147	202	188	145	2168

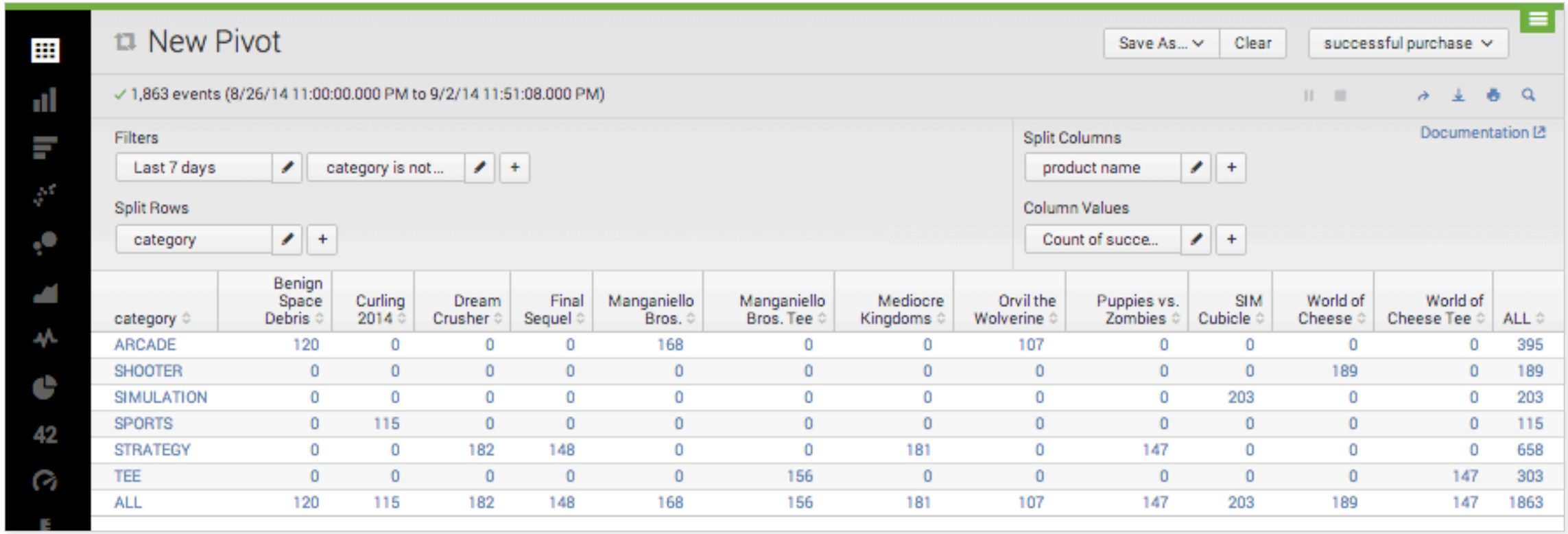
Add Additional Filters

- You can further refine your pivot by filtering on field/value pairs
  - You can think of 'split by' in rows and columns as **fields**, and 'filters' as **field=value** pairs or field value (=, <, >, !=, *)
- In this example, the report is filtered to exclude the ACCESSORIES category
  - Notice that **is not** is selected in the Match field



Filtered Pivot

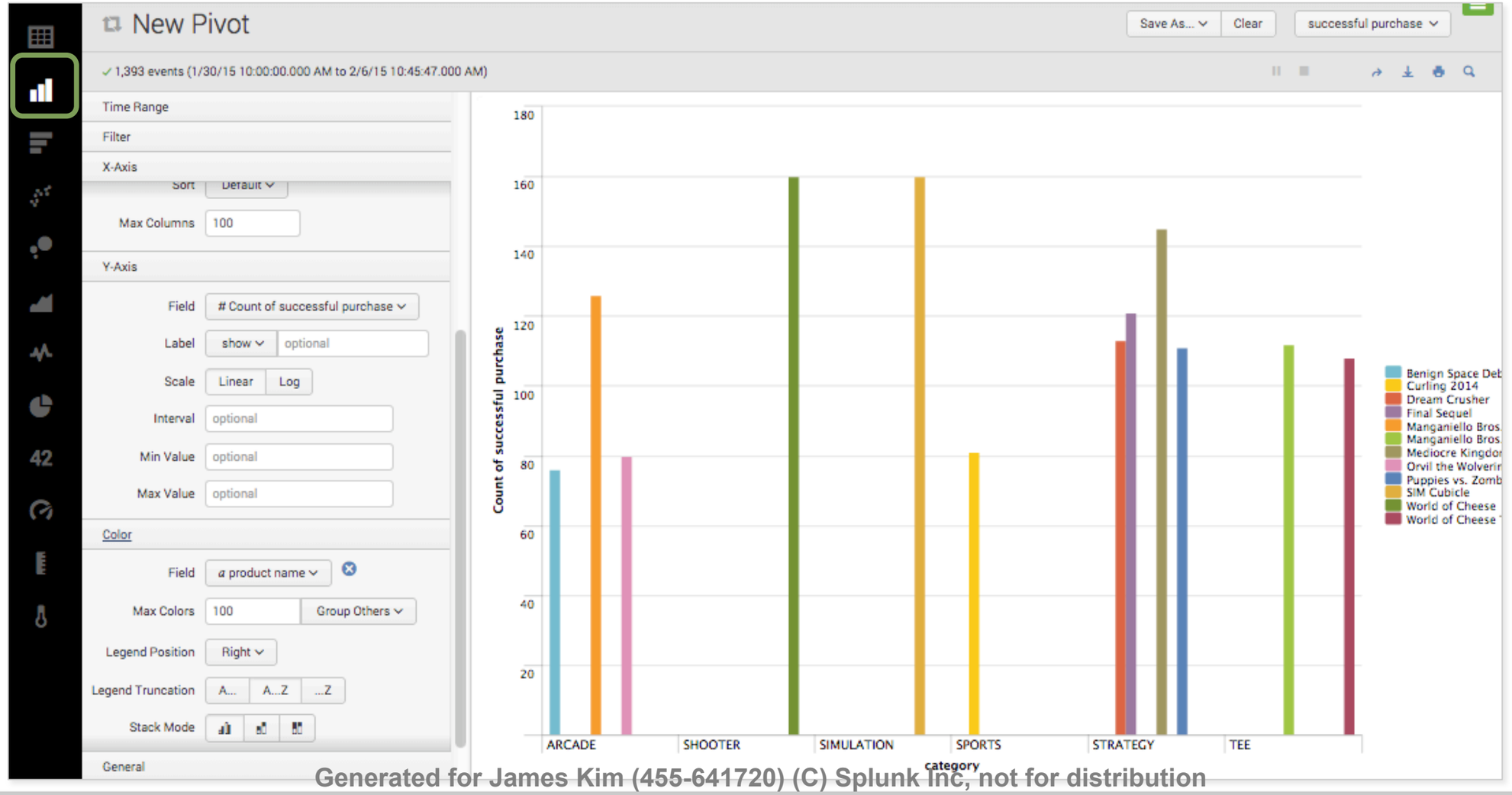
Accessories were filtered out. Only the game categories and tees appear.



category	Benign Space Debris	Curling 2014	Dream Crusher	Final Sequel	Manganiello Bros.	Manganiello Bros. Tee	Mediocre Kingdoms	Orvil the Wolverine	Puppies vs. Zombies	SIM Cubicle	World of Cheese	World of Cheese Tee	ALL
ARCADE	120	0	0	0	168	0	0	107	0	0	0	0	395
SHOOTER	0	0	0	0	0	0	0	0	0	0	189	0	189
SIMULATION	0	0	0	0	0	0	0	0	0	203	0	0	203
SPORTS	0	115	0	0	0	0	0	0	0	0	0	0	115
STRATEGY	0	0	182	148	0	0	181	0	147	0	0	0	658
TEE	0	0	0	0	0	156	0	0	0	0	0	147	303
ALL	120	115	182	148	168	156	181	107	147	203	189	147	1863

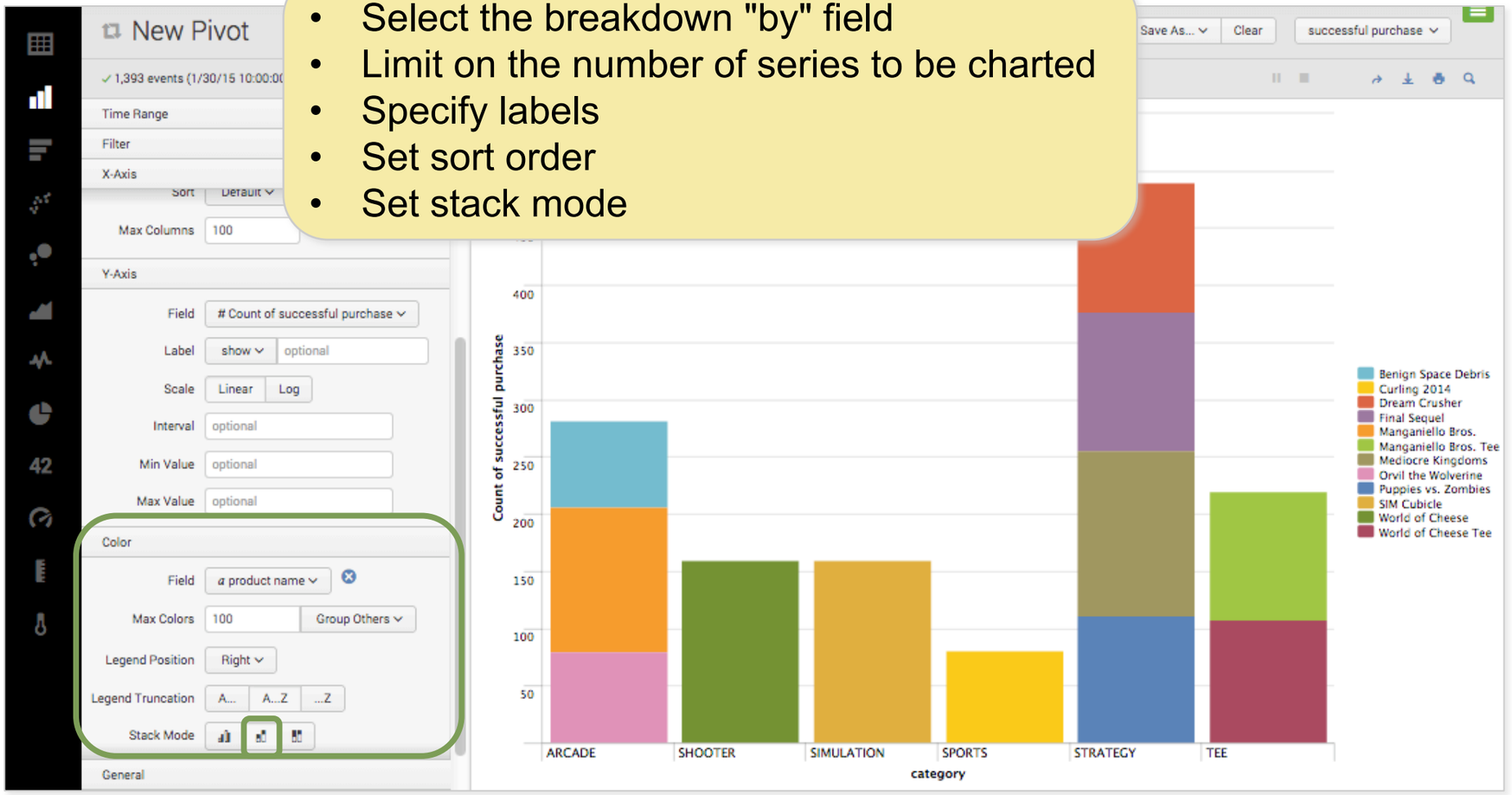
Select a Visualization Format

You can display your pivot as a table or a visualization, such as column chart



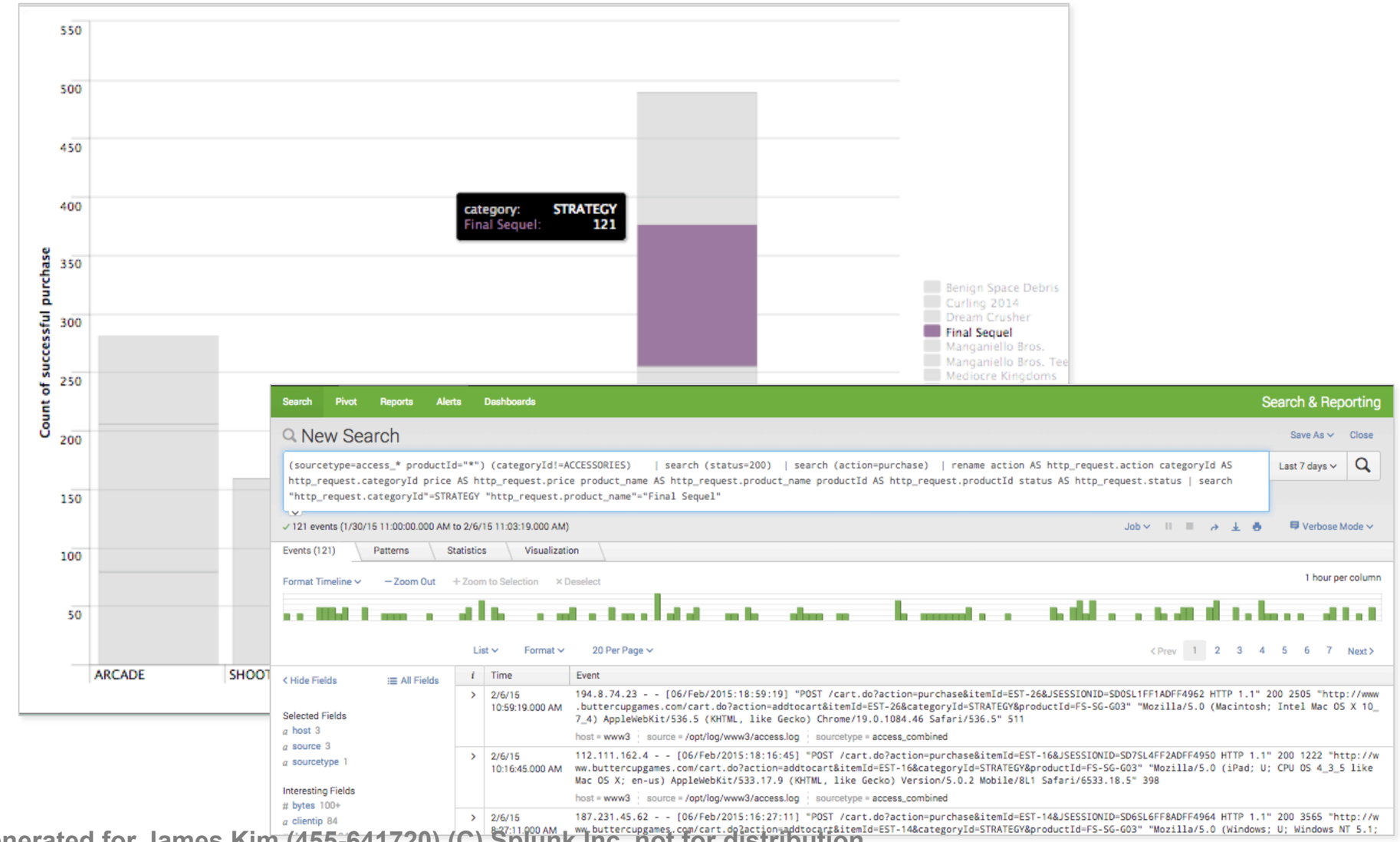
Modify Visualization Settings

- Notice along the left there are controls that allow you to change visualization settings
- By default, Drilldown is enabled, which means that when an item in the visualization is clicked, its underlying search opens in the Search and Reporting app



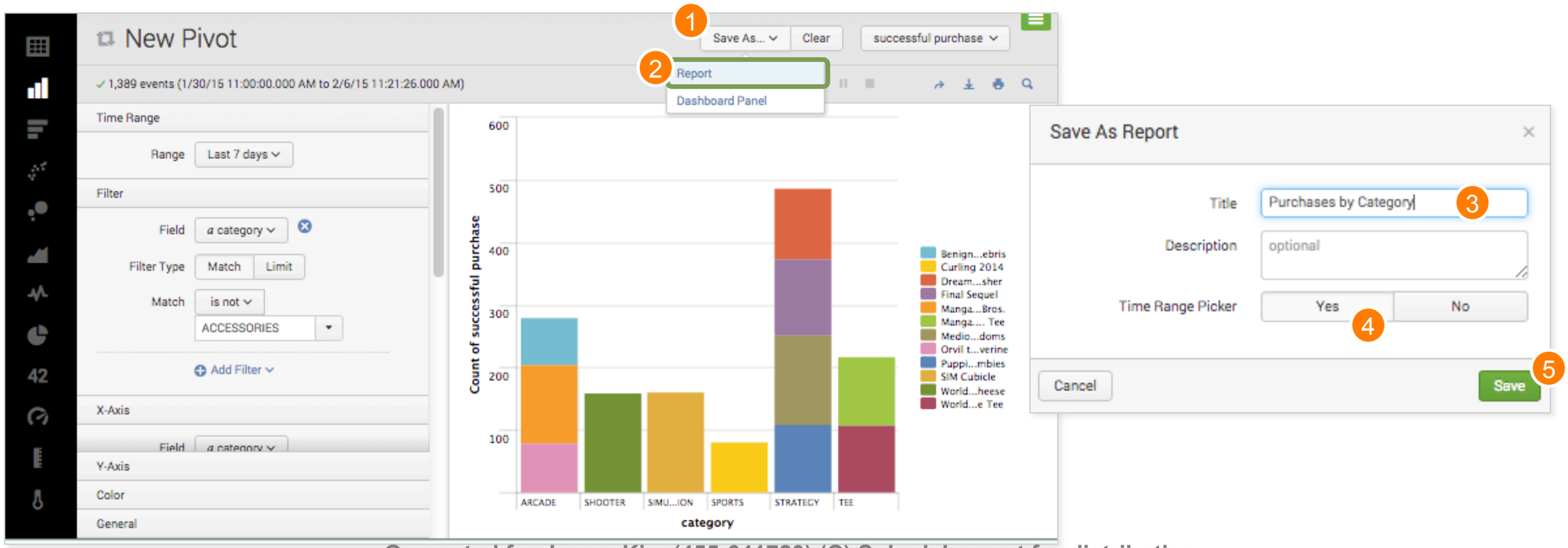
Mouse Actions

- Mouse over to reveal details
- Click an area to open its underlying search (click is available only if Drilldown remains enabled)



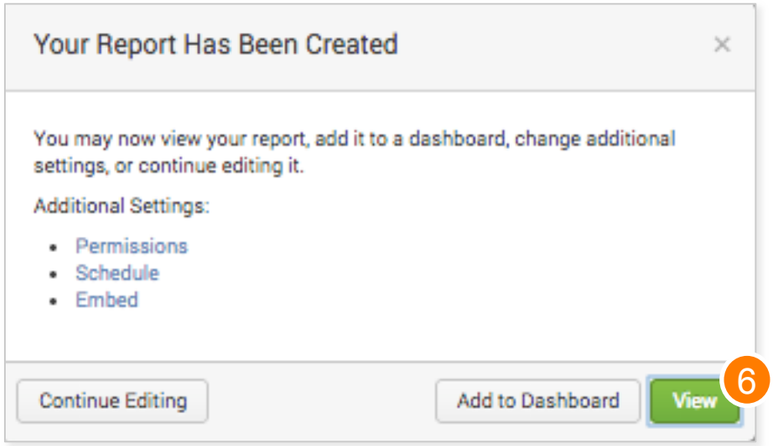
Save Pivot

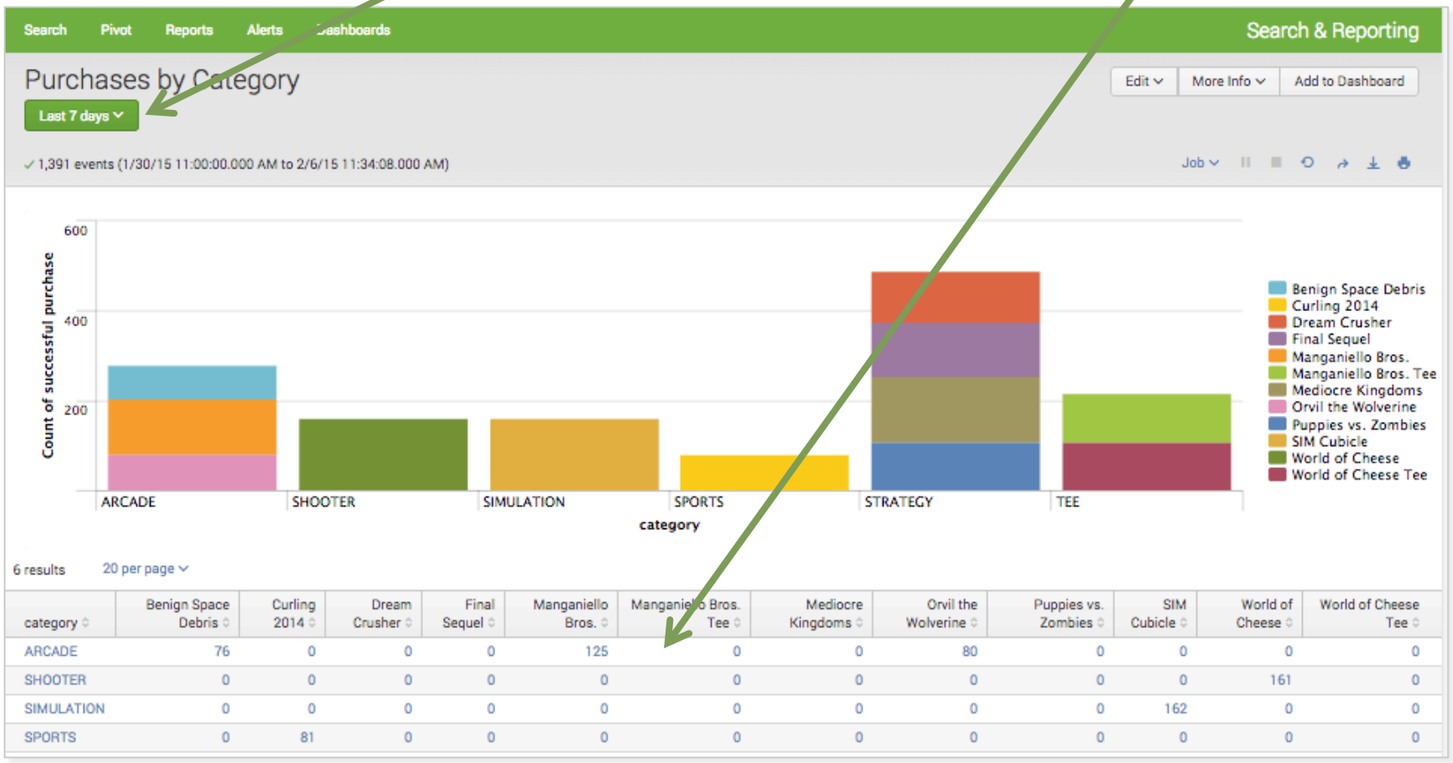
- Pivots are saved as reports or dashboard panels (both taught later in this course)
- You can choose to include a Time Range Picker in the report to allow people who view it to change the time range (default is Yes)



Save Pivot (cont.)

- Other report options will be covered later in this course (set permissions, embed, edit, or add to a dashboard)
- Click **View**. Note the report includes a Time Range Picker and a statistics table below the chart

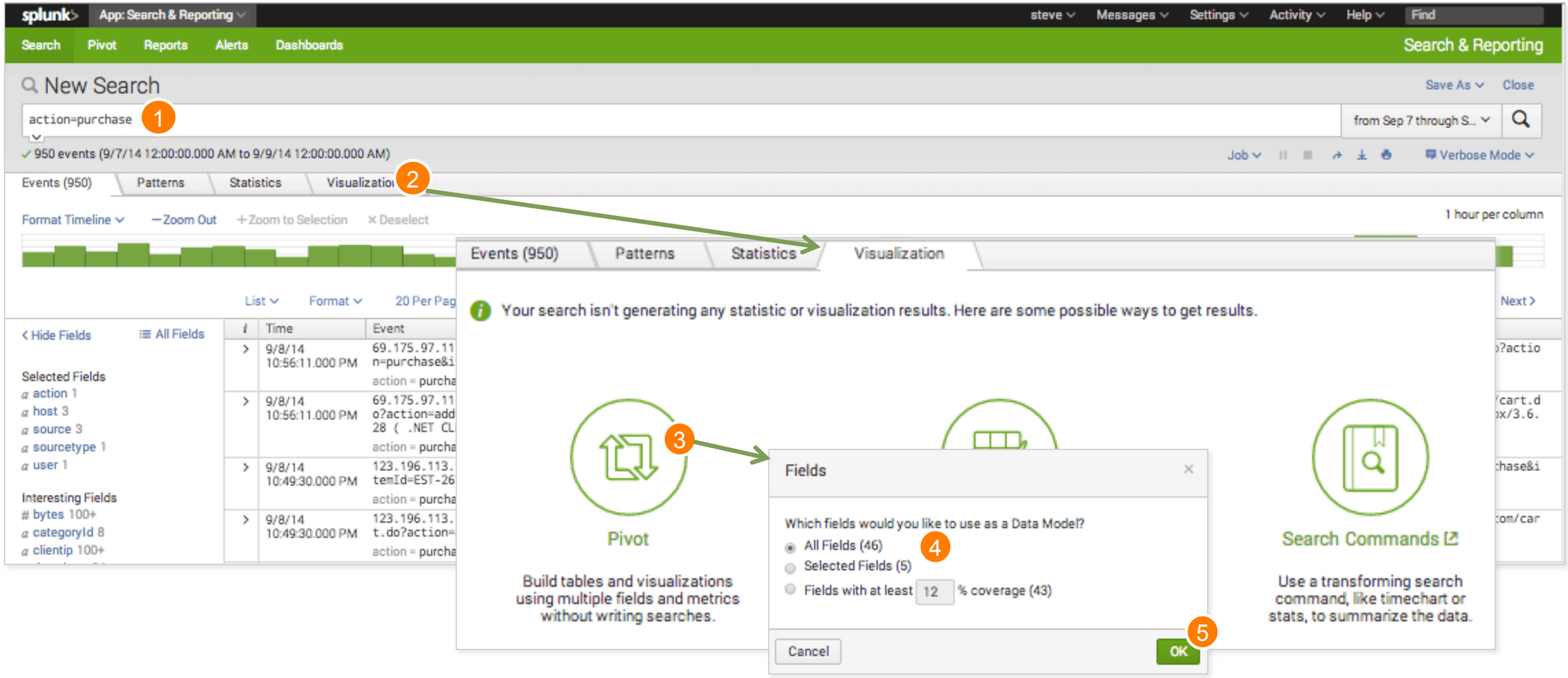




Instant Pivot Overview

- A tool that allows non-technical users to more easily get stats, tables, or visualizations from searches and create reports and dashboards
  - In previous versions of Splunk, you needed to design a data model before being able to use pivot, which required a lot of effort and Splunk expertise
  - Instant pivot automatically builds its own underlying data model with one search-based object on which the report /dashboard is based
- How to create an Instant Pivot
  1. Execute a basic search
  2. Click the **Visualization** or **Statistics** tab and click **Pivot**
  3. Select the fields you with to include in the object
  4. Create a table or visualization in Pivot and save it

Open Instant Pivot



Wrap Up

- Understand the uses of Splunk
- Define Splunk apps
- Learn basic navigation in Splunk
- Search
  - By keywords and booleans
  - By time
  - By fields
  - All of the above
- Refine searches
  - Click to add/remove terms
  - Use timeline, time modifiers, fields
- Save search results
- Create reports and charts
- Use pivots
- Create and modify dashboards and dashboard panels

Support Programs

Community:

- **Splunkbase Answers:** answers.splunk.com
  Post specific questions and get them answered by Splunk community experts.
- **Splunk Docs:** docs.splunk.com
  These are constantly updated. Be sure to select the version of Splunk you are using.
- **Wiki:** wiki.splunk.com
  A community space where you can share what you know with other Splunk users.
- **IRC Channel:** #splunk on the EFNet IRC server Many well-informed Splunk users “hang out” here.