



# Using Splunk

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Course Outline

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

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Introducing Splunk's User Interface

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Module Objectives

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

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

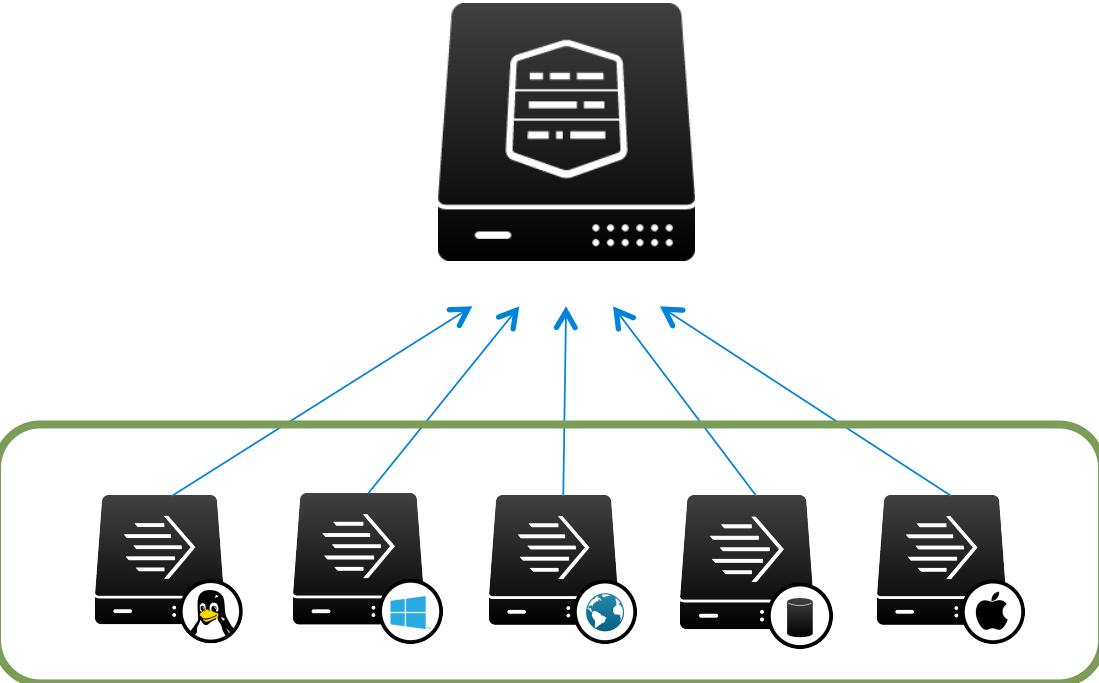
# Got Data?



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



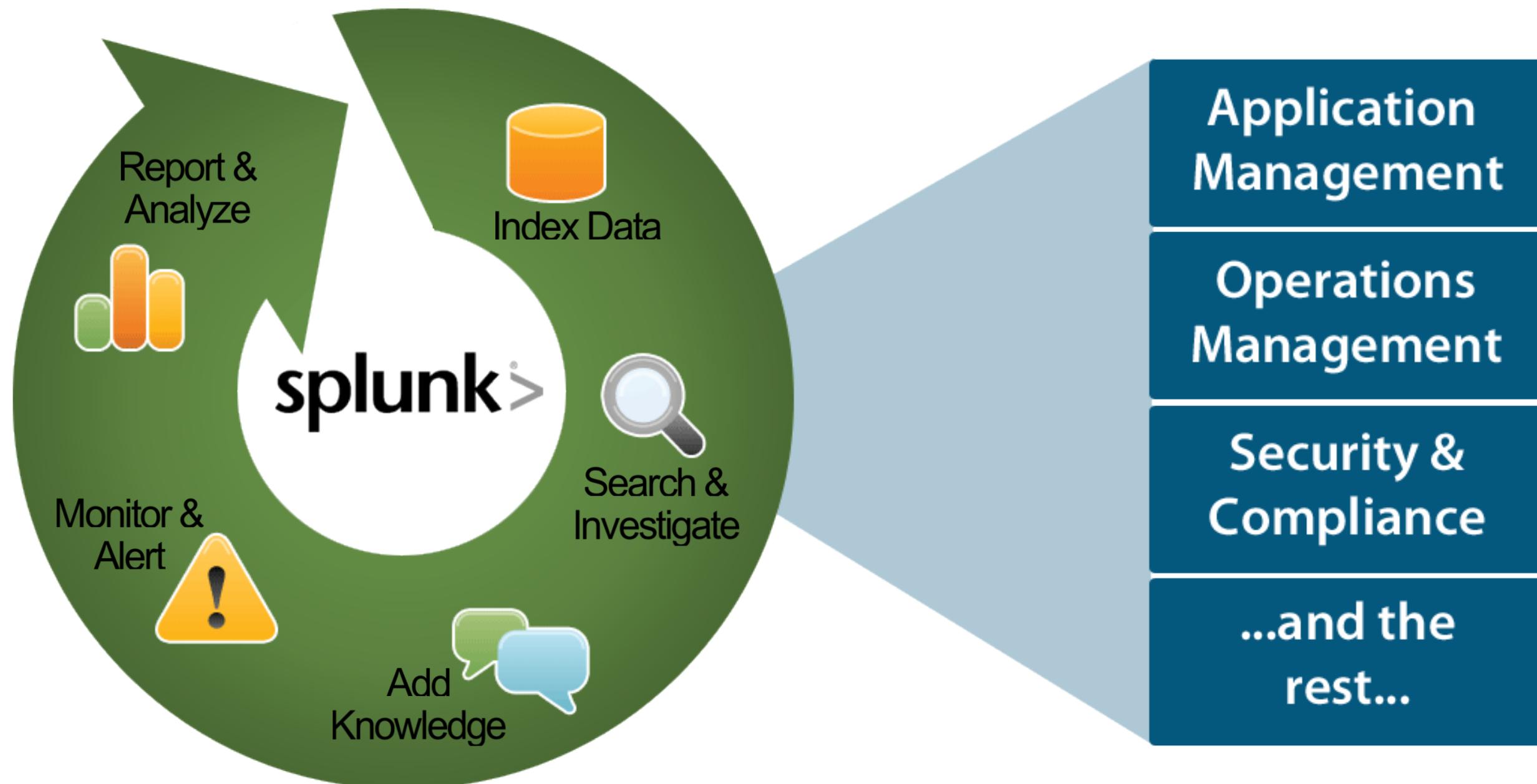
- Logs
- Configurations
- Messages
- Call detail records
- Clickstream
- Alerts
- Metrics
- Scripts
- Changes
- Tickets
- **Any data**



Indexes any data from any source

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

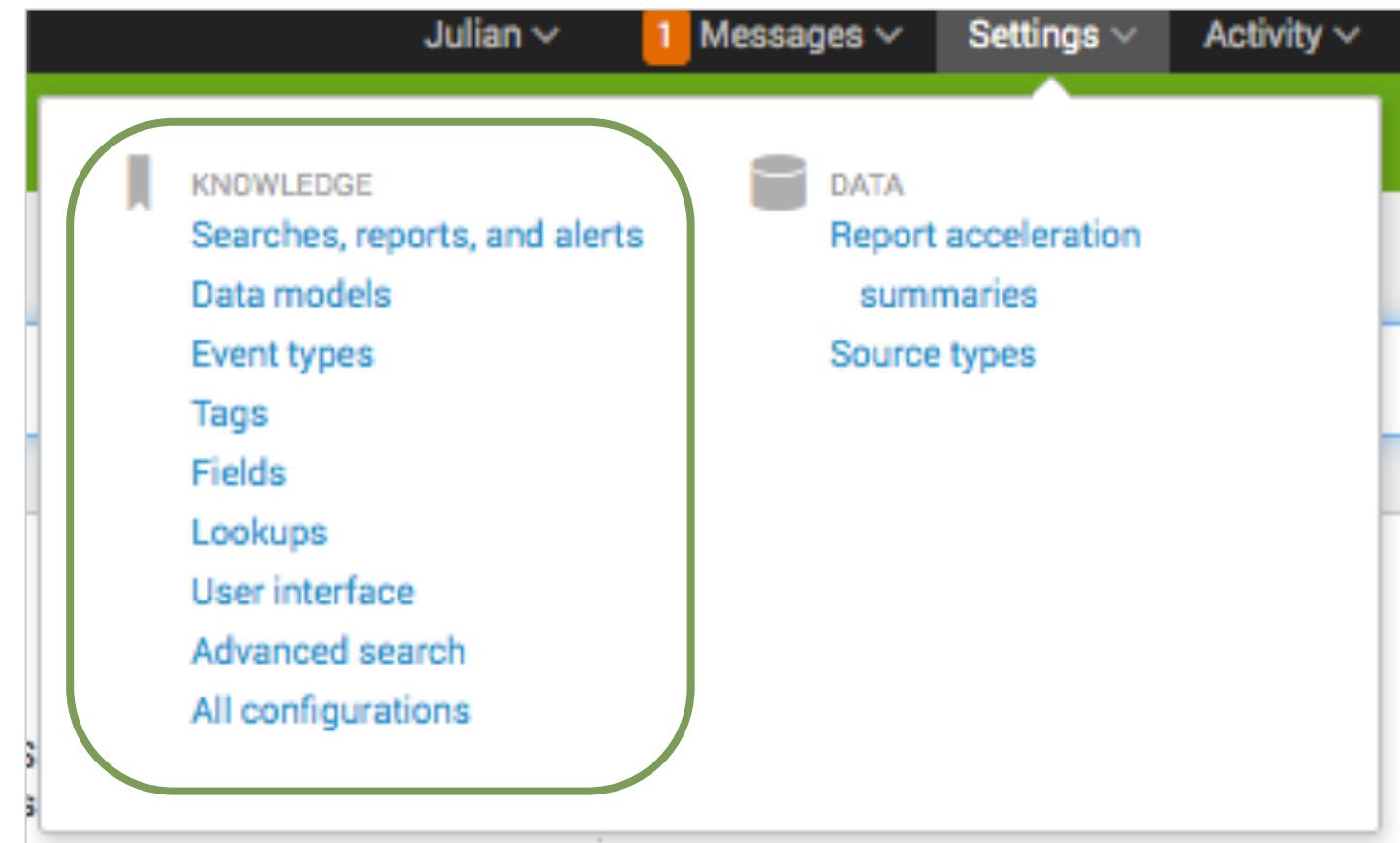
# One Splunk. Many Uses.



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

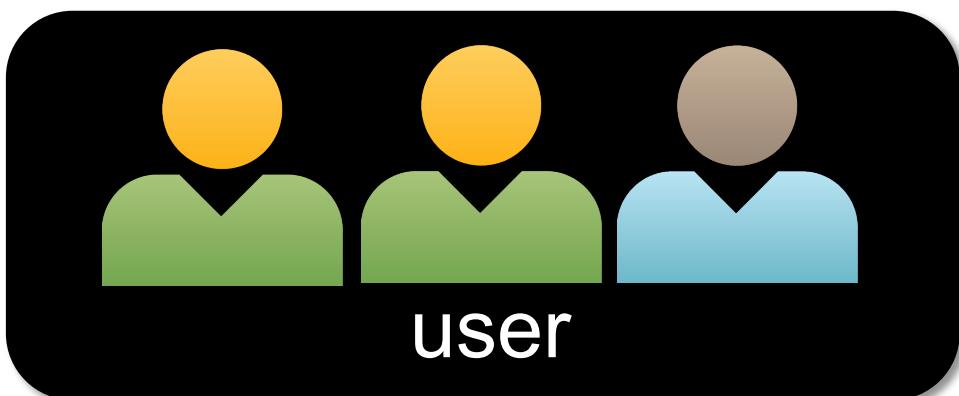
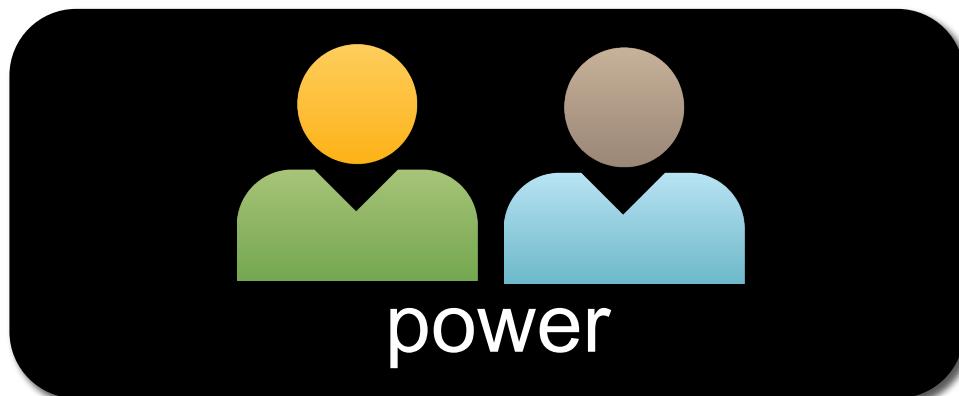


[http://docs.splunk.com/Documentation/Splunk/latest/  
Knowledge/WhatIsSplunkknowledge](http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/WhatIsSplunkknowledge)

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

The screenshot shows the Splunk User Settings interface. At the top, there is a navigation bar with links for 'splunk', 'Apps', 'steve' (highlighted with a green box and orange circle 1), 'Messages', 'Settings', 'Activity', and 'Help'. Below the navigation bar, the user's name 'steve' is displayed, along with a 'Logout' link. A dropdown menu is open over the 'steve' link, showing options: 'Edit Account' (highlighted with a green box and orange circle 2) and 'Logout'. The main content area is titled 'Edit Account' for the user 'steve'. It contains several input fields and dropdown menus:

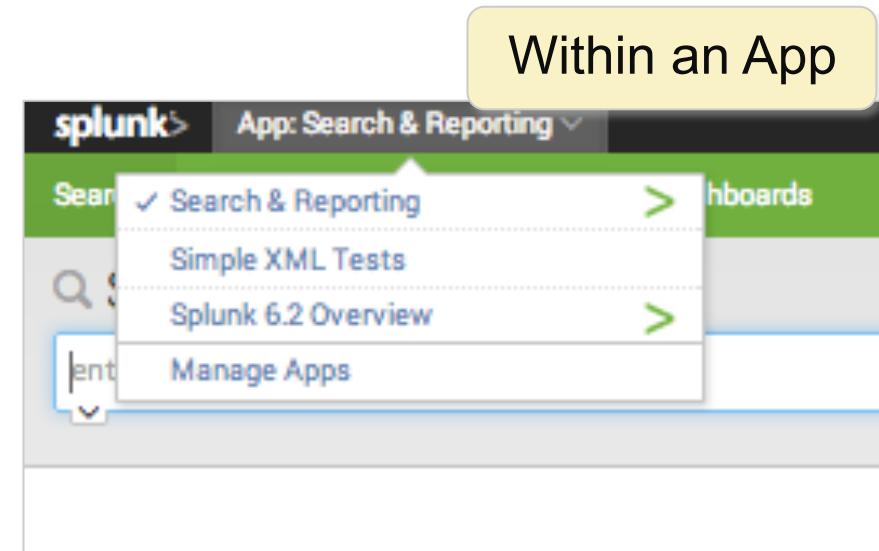
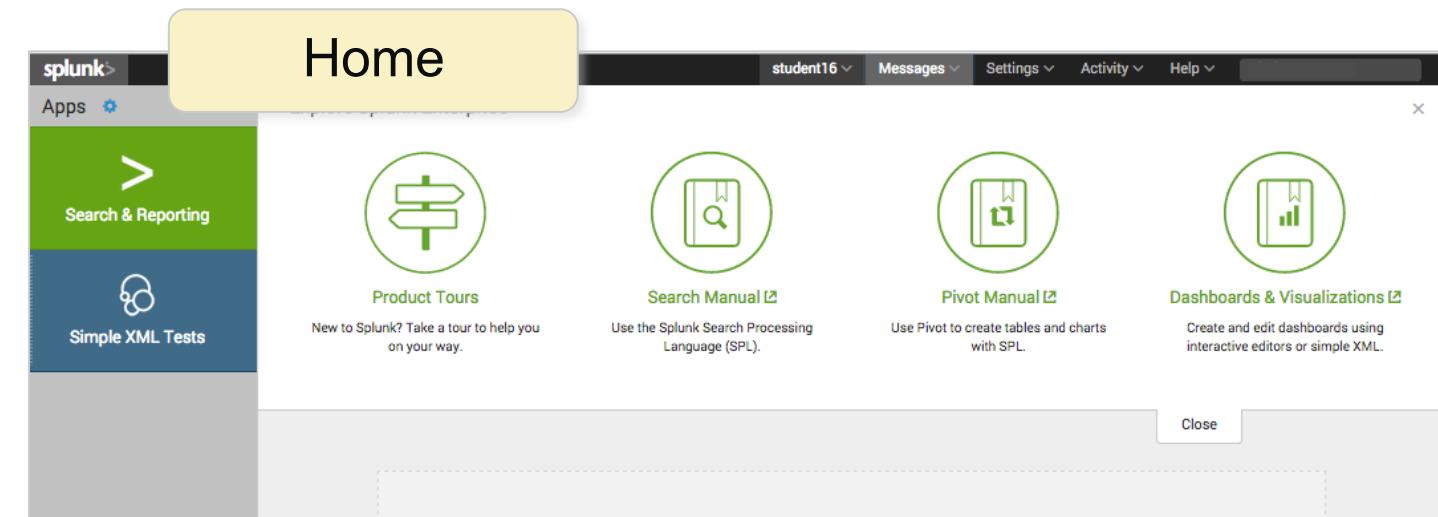
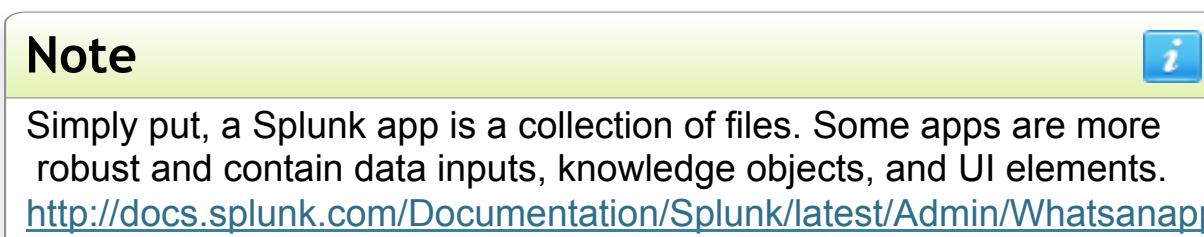
- Full name:** An input field containing the value '3' (highlighted with orange circle 3).
- Email address:** An empty input field.
- Time zone:** A dropdown menu set to 'Default System Timezone --' (highlighted with orange circle 4). A tooltip below it says 'Set a time zone for this user.'
- Default app:** A dropdown menu set to 'class\_SnR' (highlighted with orange circle 5). A tooltip below it says 'Set a default app for this user. This will override any default app inherited from this user's roles.' There is also a checked checkbox labeled 'Restart backgrounded jobs' with a tooltip 'Should backgrounded jobs be restarted when Splunk is restarted.'
- Set password:** A section with two input fields for 'Password' and 'Confirm password' (highlighted with orange circle 6).

A 'Cancel' button is at the bottom left, and a 'Save' button is at the bottom right.

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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>



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Home app

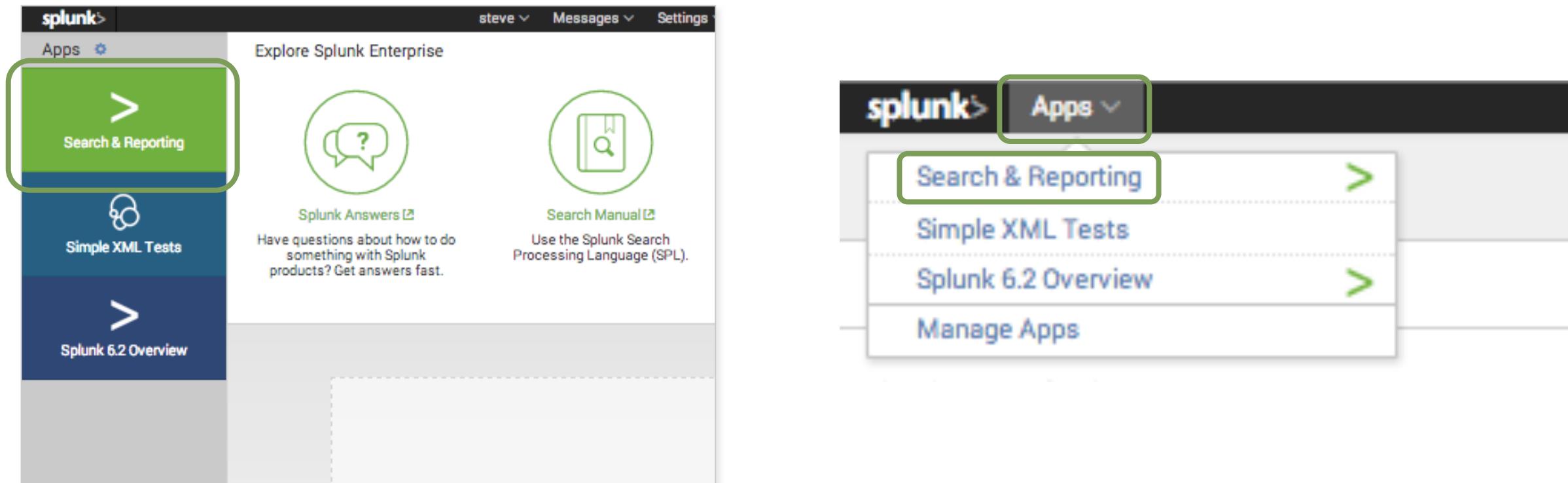
Click the Splunk logo to return to the app that was set as your default app; the default is the Home app

The screenshot shows the Splunk Home app interface. On the left, a sidebar titled "Explore Splunk Enterprise" lists three items: "Search & Reporting", "Simple XML Tests", and "Splunk 6.2 Overview". A green arrow points from the text above to the "splunk>" logo in the top left corner of the sidebar. On the right, there is a "Help" section with four links: "Splunk Answers" (with a question mark icon), "Search Manual" (with a book icon), "Pivot Manual" (with a book icon), and "Dashboards & Visualizations" (with a bar chart icon). A yellow callout box labeled "Links to several help resources" points to the "Search Manual", "Pivot Manual", and "Dashboards & Visualizations" links. Below the help section, there is a dashed-line box containing six small dashboard icons. A yellow callout box labeled "Once you've built dashboards with your data, you can choose one to appear in your Home app" points to these icons. The text "Choose a home dashboard" is centered below the icons.

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

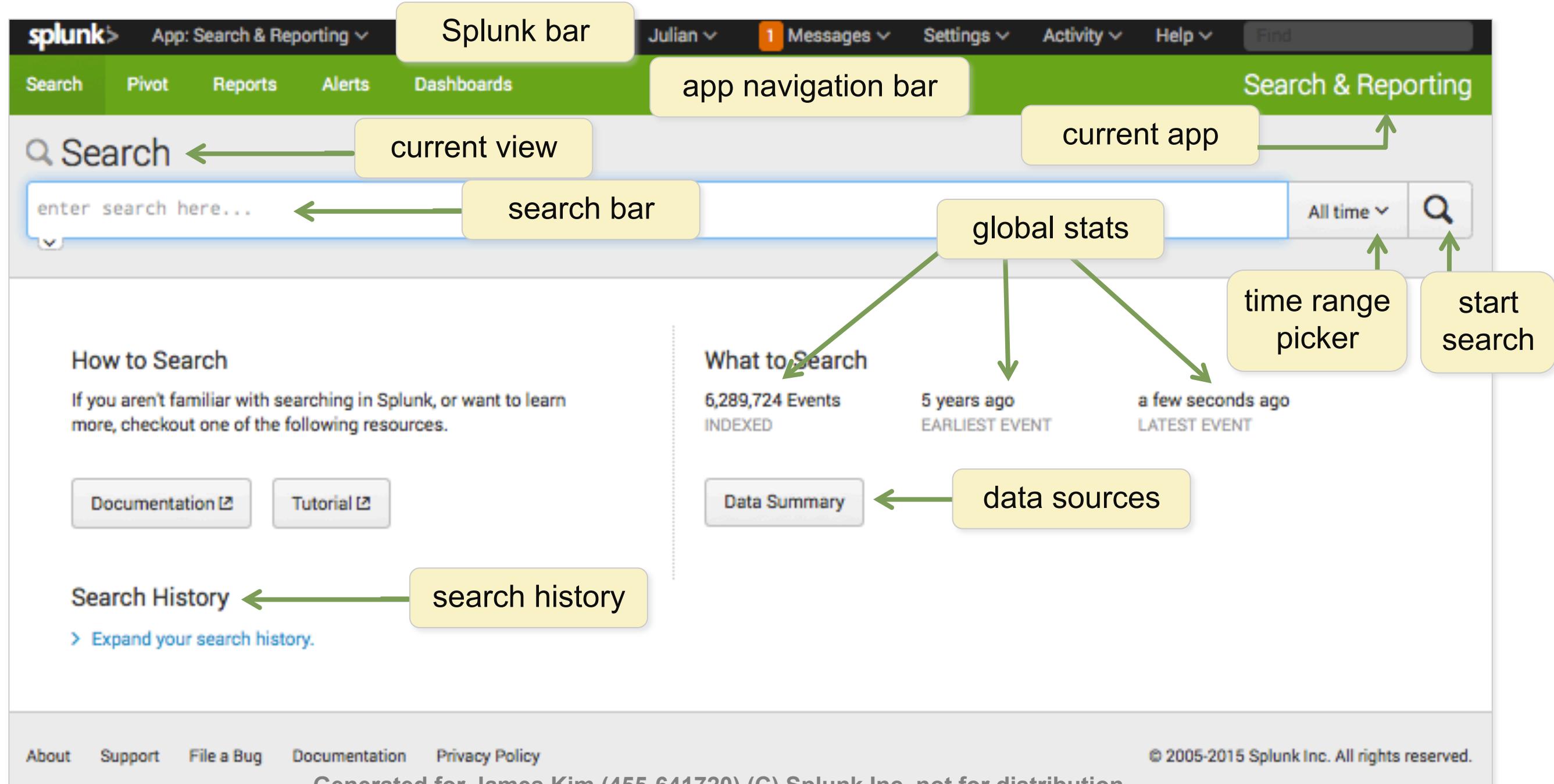
# Search & Reporting App Overview

- 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**



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Search & Reporting App Overview (cont.)



# Data Summary Views

The screenshot shows the Splunk interface with the 'Search & Reporting' app selected. A yellow callout box points to the 'Data Summary' button in the bottom right corner of the search bar. Three green arrows point from the definitions below to the corresponding tabs in the Data Summary interface: 'Hosts (10)' (Host), 'Sources (16)' (Source), and 'Sourcetypes (11)' (Sourcetype). The Data Summary interface displays lists of hosts, sources, and sourcetypes with their respective counts and last update times.

Shows hosts, sources, sourcetypes on separate tabs – you can also filter the lists

- **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

Sourcetype	Count	Last Update
access_combined	376,985	9/2/14 10:52:14.000 PM
cisco_esa	48,137	9/2/14 10:54:08.000 PM
cisco_firewall	1,159	9/2/14 5:37:02.000 PM
cisco_wsa_squid	26,697	9/2/14 10:53:42.000 PM
history_access	19,400	9/2/14 5:37:02.000 PM
linux_secure	152,194	9/2/14 10:54:04.000 PM
ps	47,351	9/2/14 10:53:57.000 PM
sales_entries	545,943	9/2/14 10:53:43.000 PM
sendmail_syslog	17,378	9/2/14 10:43:36.000 PM
vendor_sales	199,220	9/2/14 10:39:08.000 PM
winauthentication_security	26,737	9/2/14 5:37:02.000 PM

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Key Details

The screenshot shows the Splunk interface with the following elements:

- Top Bar:** splunk> App: Search & Reporting, steve, Messages, Settings, Activity, Help.
- Search Bar:** Search term: error OR fail\* NOT sourcetype=ps, Results: 146,307 events (before 9/2/14 7:16:58.000 PM), Search & Reporting tab selected.
- Note Panel:** Note: Learn more about Splunk from Splunk's online glossary, the Splexicon at <http://docs.splunk.com/Splexicon>.
- Event View:** Statistics and Visualization tabs are available. The visualization shows a histogram of events over time. The event list table has columns: Time, Event. The first event is highlighted:

Time	Event
9/2/14 7:16:41.000 PM	Tue Sep 02 2014 19:16:41 www1 sshd[3461]: Failed password for jira from 64.120.15.156 port 4012 ssh2 host = www1   source = /opt/log/www1/secure.log   sourcetype = linux_secure
- Selected Fields:** host 7, source 11, sourcetype 6.
- Interesting Fields:** action 4, app 1, date\_hour 24, date\_mday 31, date\_minute 60.
- Event Detail:** A callout highlights the first event in the list, showing the Field and Field value for host.

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Searching

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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 insensitive
- 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

The image shows a grid of search queries, each consisting of a search bar and a search button. The queries are:

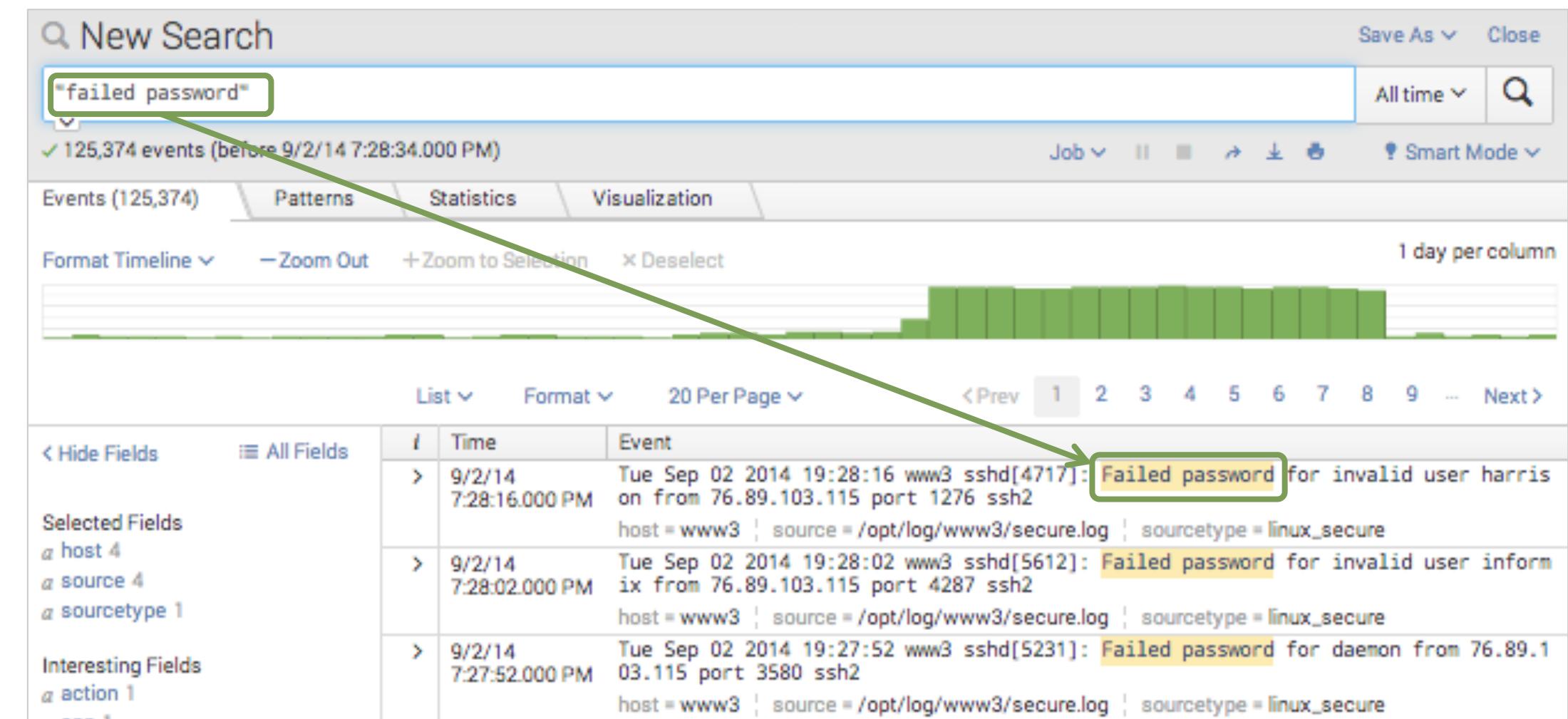
- fail
- fail\*
- fail\* nfs
- error OR 404
- error OR failed AND 500 OR 503
- error OR (failed AND (500 OR 503))
- "login failure"
- host !=www3
- price>500

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Search Results

Matching results are returned immediately

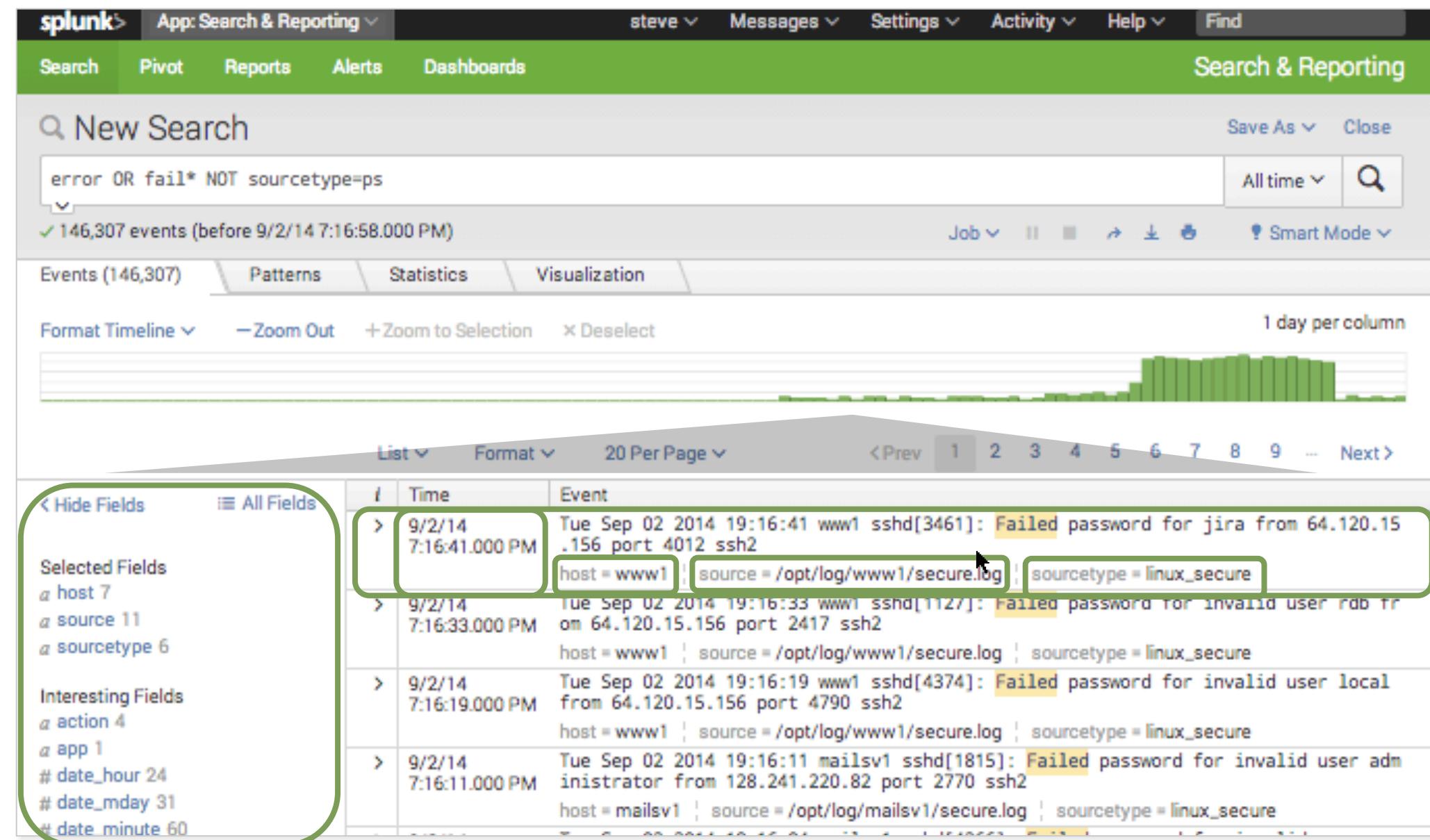
- Displayed in reverse chronological order (newest first)
- Matching search terms are highlighted



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Event Details

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

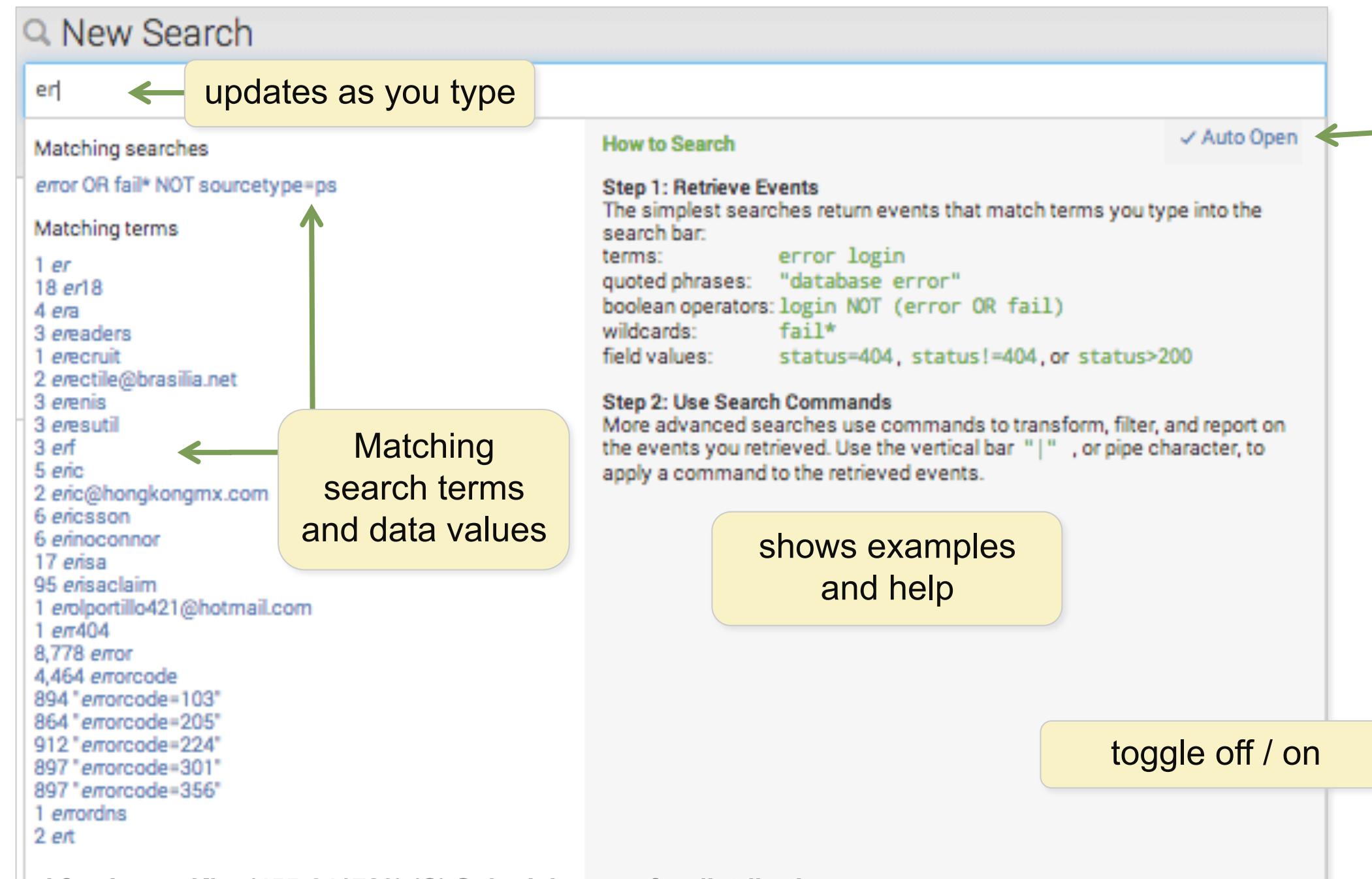


Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Search Results Details

The screenshot shows the Splunk search interface with various UI elements annotated:

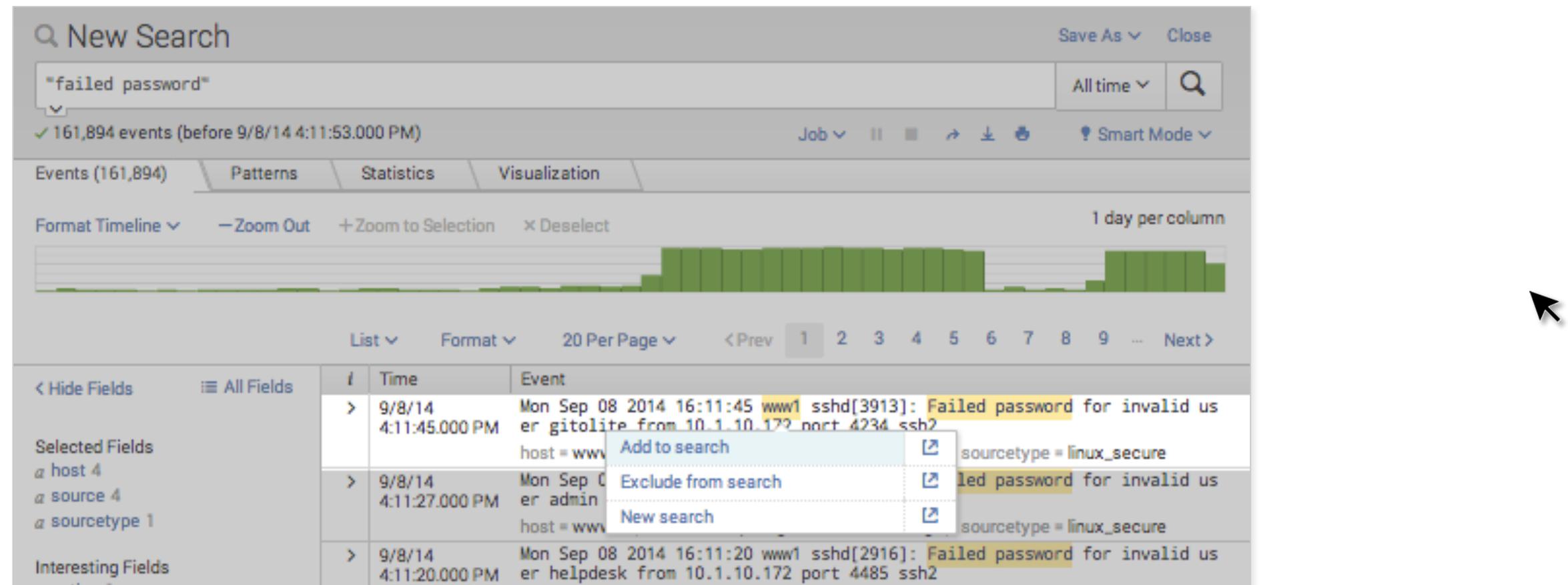
- New Search**: The search bar at the top left.
- time range picker**: The dropdown menu for setting the time range, with "All time" selected.
- Events (125,374)**: The count of events found, located below the search bar.
- Results typically appear in the Events tab**: A tooltip pointing to the Events tab in the navigation bar.
- search mode**: The search mode dropdown in the top right.
- timeline**: The timeline visualization showing event density over time.
- paginator**: The pagination controls at the bottom of the search results.
- Fields sidebar**: The sidebar on the left listing available fields.
- timestamp**: The timestamp field highlighted in the Fields sidebar.
- selected fields**: The timestamp field listed under the "Selected Fields" section in the search results.
- events**: The main list of search results, showing log entries related to failed password attempts.

I	Time	Event
>	9/2/14 7:28:16.000 PM	Tue Sep 02 2014 19:28:16 www3 sshd[4717]: Failed password for invalid user harris on from 76.89.103.115 port 1276 ssh2 host = www3   source = /opt/log/www3/secure.log   sourcetype = linux_secure
>	7:28:02.000 PM	28:02 www3 sshd[5612]: Failed password for invalid user inform 15 port 4287 ssh2 host = www3   source = /opt/log/www3/secure.log   sourcetype = linux_secure
>	9/2/14 7:27:52.000 PM	Tue Sep 02 2014 19:27:52 www3 sshd[5231]: Failed password for daemon from 76.89.1 03.115 port 3580 ssh2 host = www3   source = /opt/log/www3/secure.log   sourcetype = linux_secure

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** Contains the query `"failed password"`, a time range from `Month to date`, and a search button.
- Summary Bar:** Shows `37,697 events` from `9/1/14 12:00:00.000 AM to 9/8/14 4:48:44.000 PM`. It includes buttons for `Job`, `Events` (selected), `Patterns`, `Statistics`, `Visualization`, `Format Timeline`, `Zoom Out`, `Zoom to Selection`, `Deselect`, and `Verbose Mode`.
- Timeline Visualization:** A horizontal bar showing event times as green vertical bars. A tooltip indicates `1 hour per column`.
- List View:** The main area displays a table of search results. The table has columns for `Time` and `Event`. The first event is highlighted in yellow.

	Time	Event
< Hide Fields	All Fields	> 9/8/14 Mon Sep 08 2014 16:48:30 www2 sshd[3647]: Failed password for invalid user db2inst1 from 199.15.234.66 port 1708 ssh2 host = www2   source = /opt/log/www2/secure.log   sourcetype = linux_secure
Selected Fields	a host	> 9/8/14 Mon Sep 08 2014 16:48:14 www2 sshd[1334]: Failed password for invalid user
- Pagination:** Shows page 1 of 9.

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Select a Specific Time

The screenshot shows the Splunk search interface with various time range selection methods:

- Relative:** Earliest: 0 Seconds Ago, Latest: now, Beginning of today (9/8/14 8:27:31.000 PM), Apply button.
- Real-time:** Earliest: Seconds Ago, Latest: now, Apply button.
- Date Range:** Before: 09/08/2014, Apply button.
- Date & Time Range:** Earliest: 01/01/1970 00:00:00.000, Latest: 09/08/2014 17:24:47.000, Apply button.
- Advanced:** Earliest: 1/1/70 12:00:00.000 AM, Latest: 9/8/14 4:11:37.000 PM, Apply button, Documentation link.

A green bracket on the left groups the first four methods under "custom time ranges". A green bracket on the right groups the last three methods under "preset time ranges".

**Presets:**

- Real-time:
  - 30 second window
  - 1 minute window
  - 5 minute window
  - 30 minute window
  - 1 hour window
  - All time (real-time)
- Relative:
  - Today
  - Week to date
  - Business week to date
  - Month to date
  - Year to date
  - Yesterday
  - Previous week
  - Previous month
  - Previous year
- Other:
  - Last 15 minutes
  - Last 60 minutes
  - Last 4 hours
  - Last 24 hours
  - Last 7 days
  - Last 30 days

**custom time ranges**

**preset time ranges**

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Specifying Time in Search Text

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

The screenshot shows the Splunk interface with a search bar containing the query: `action=purchase earliest=-7d@w1 latest=@w6`. The search results show 2,554 events from before August 1, 2015, 12:00:00.000 AM. The interface includes a timeline visualization at the top and a detailed list of events below. The list shows three entries:

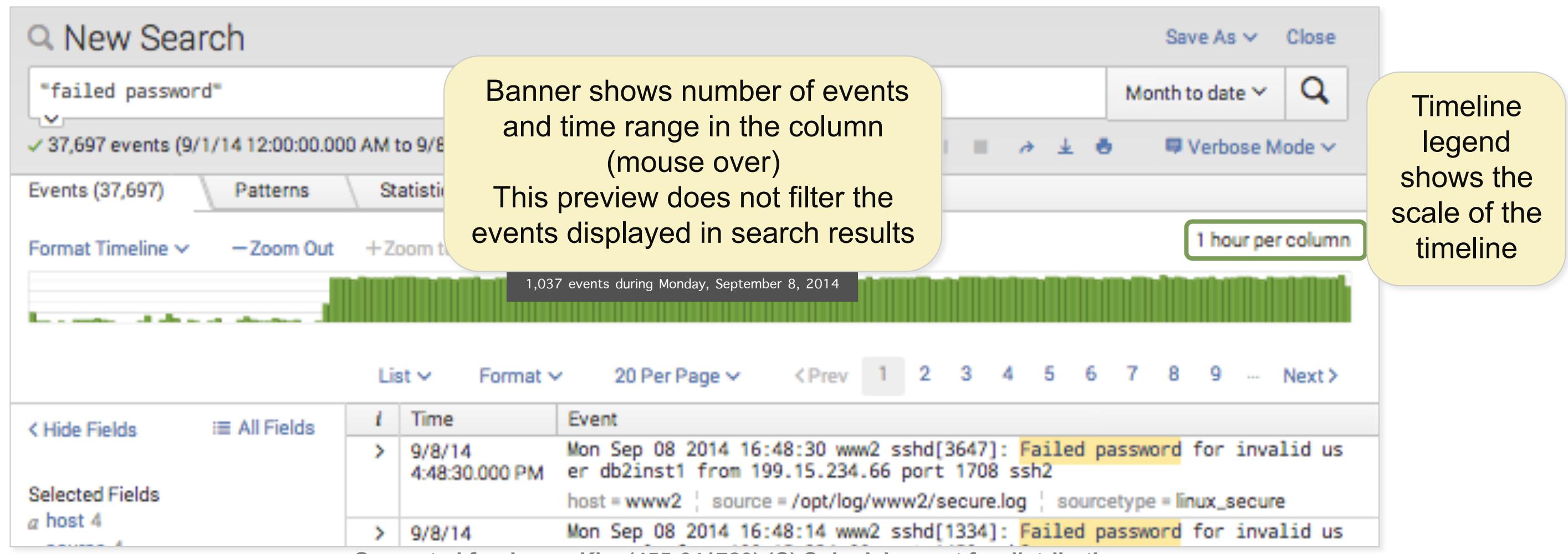
	Time	Event
>	7/31/15 11:48:28.000 PM	59.162.167.100 - - [01/Aug/2015:06:48:28] "POST /cart/error.do?msg=CreditNotAccepted&JSESSIONID=SD0SL8FF9ADFF178948 HTTP 1.1" 200 1339 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-26" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 224 host = www2   source = /opt/log/www2/access.log   sourcetype = access_combined
>	7/31/15 11:48:26.000 PM	59.162.167.100 - - [01/Aug/2015:06:48:26] "POST /cart.do?action=purchase&itemId=EST-26&JSESSIONID=SD0SL8FF9ADFF178948 HTTP 1.1" 200 1634 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-26&categoryId=TEE&productId=WC-SH-T02" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 685 host = www2   source = /opt/log/www2/access.log   sourcetype = access_combined
>	7/31/15 11:43:05.000 PM	199.15.234.66 - - [01/Aug/2015:06:43:05] "POST /cart/error.do?msg=NothingInCart&JSESSIONID=SD6SL6FF6ADFF178931 HTTP 1.1" 200 3670 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-14" "Mozilla/5.0 (compatible; NetcraftSurveyAgent/1.0/cc-prepass-https; +info@netcraft.com)" 182 host = www1   source = /opt/log/www1/access.log   sourcetype = access_combined

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# View the Timeline

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

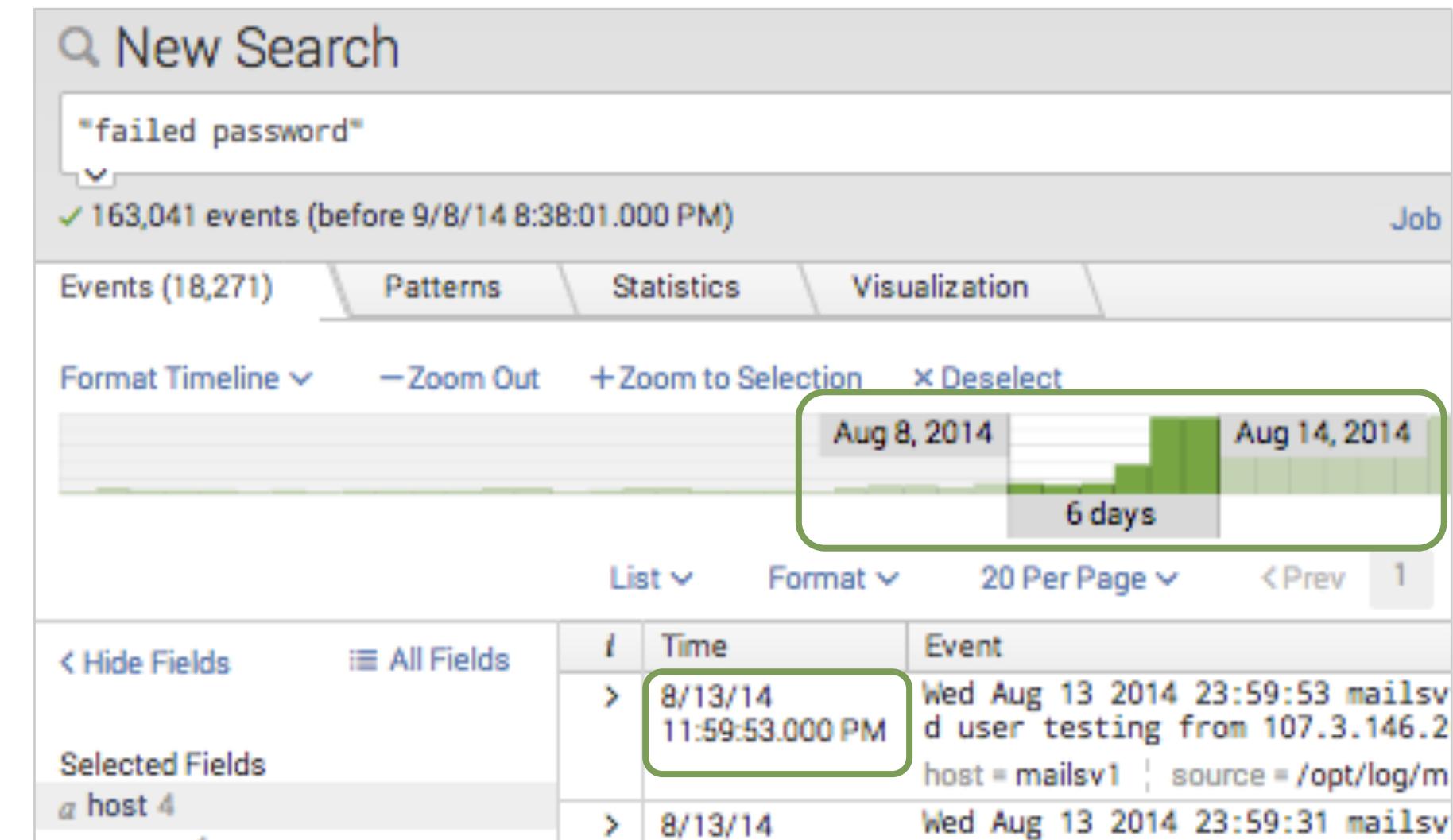
- Mouse over for details, or single-click to filter to results for that time period



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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)



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Use Other Timeline Controls

- **Format Timeline**

- Hides or shows the timeline in different views

- **Zoom Out**

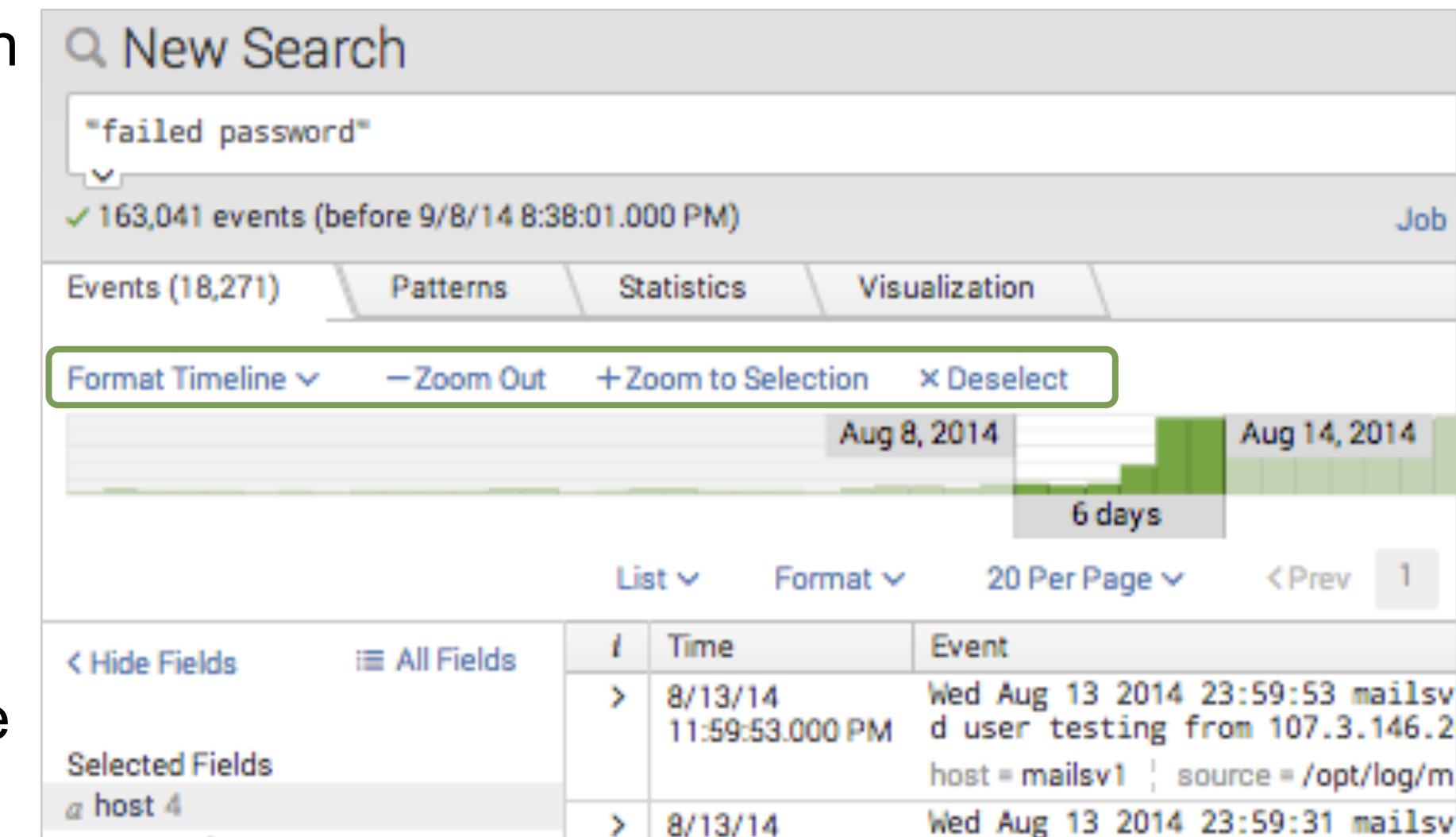
- Expands the time focus & re-runs the search

- **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

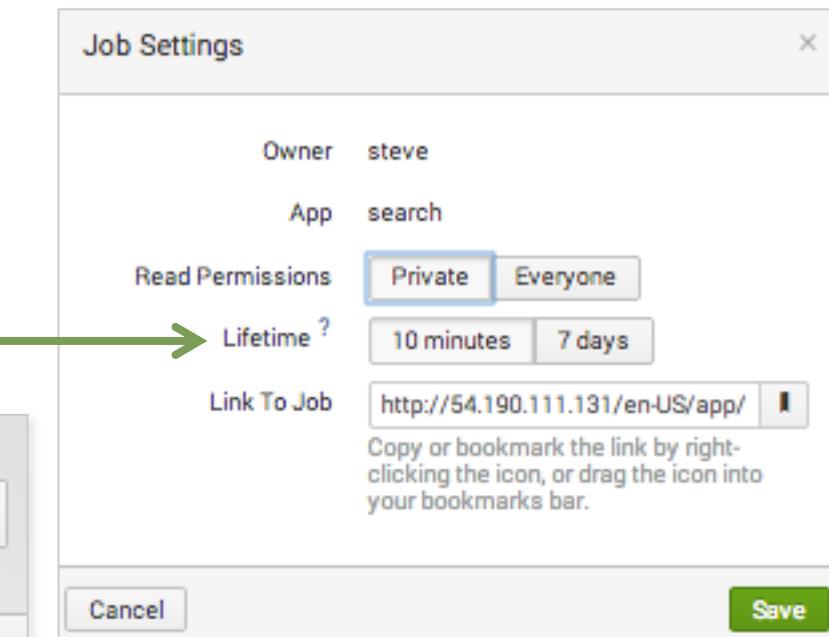
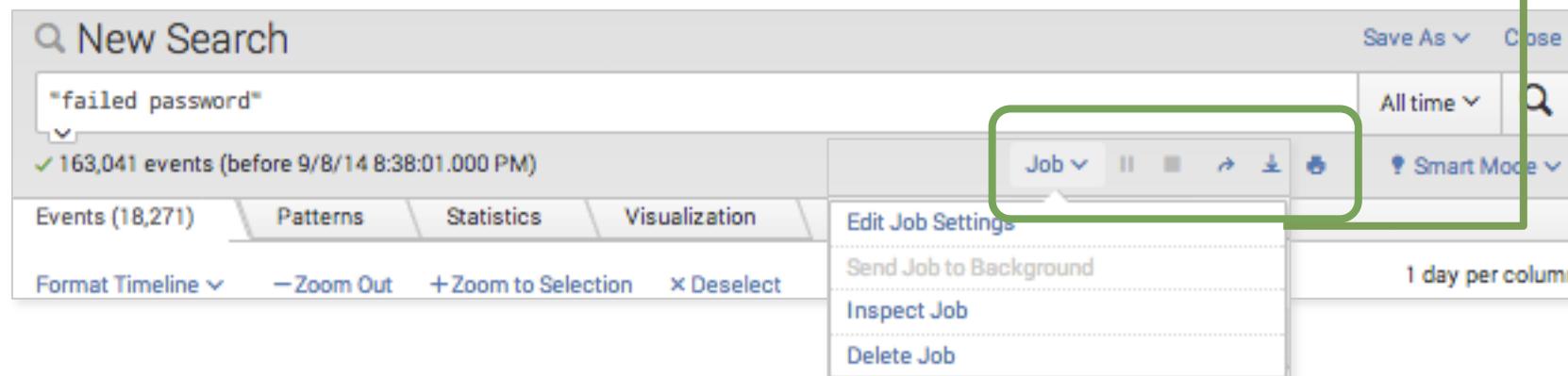


Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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)

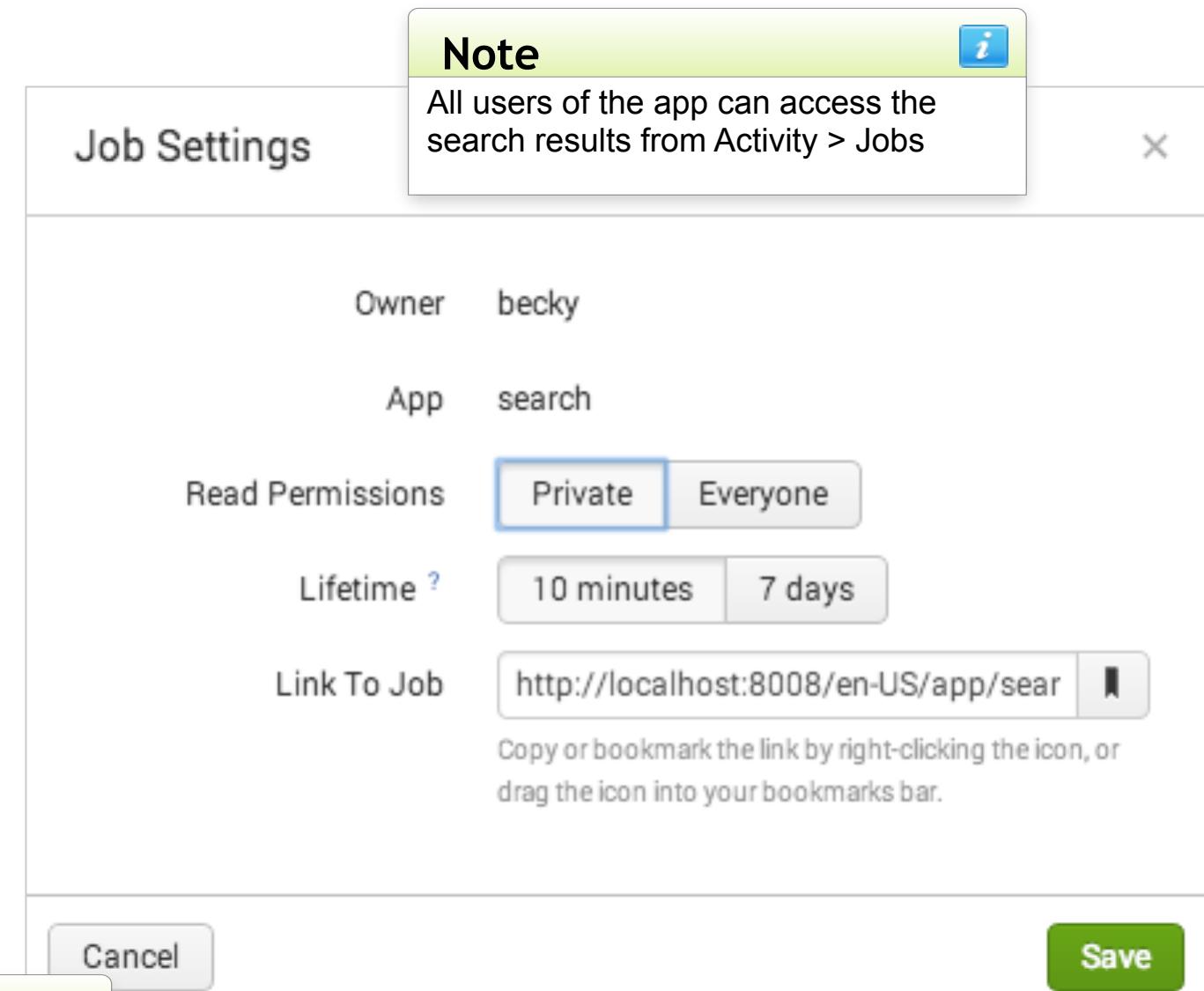
- **Pause** – toggles to resume the search
- **Stop** – finalizes the search in progress
- Jobs are available for 10 minutes (default)
- Get a link to results from the **Job** menu



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Set Permissions

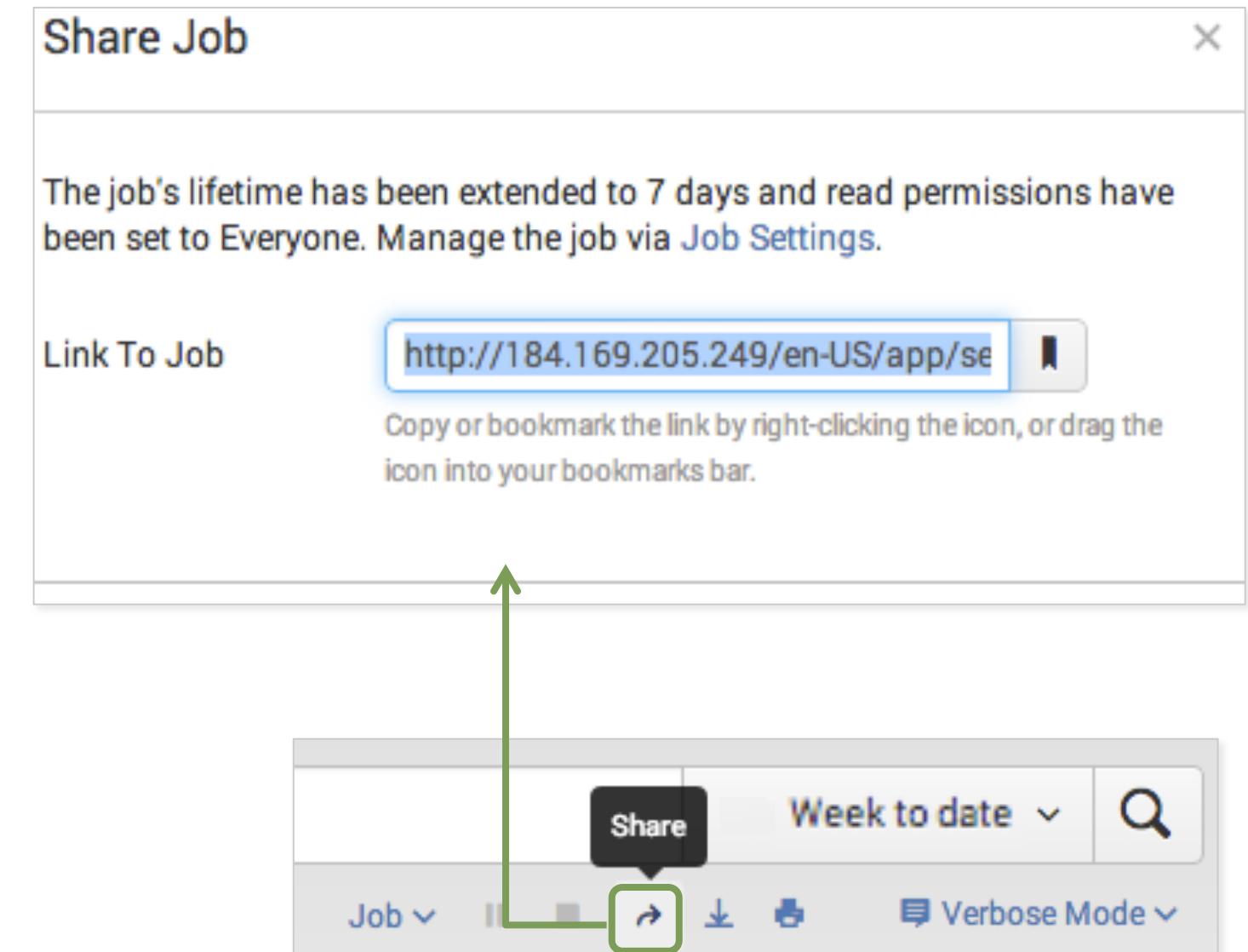
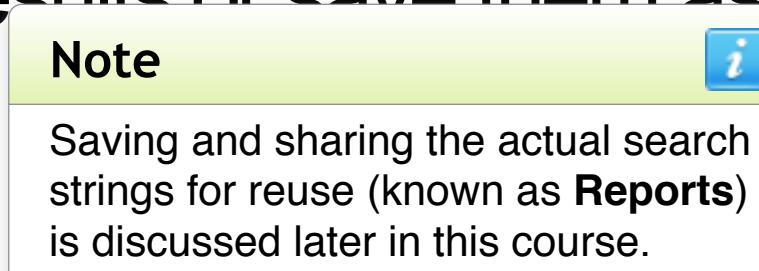
- **Private [default]**
  - Only the creator can access
- **Everyone**
  - (All Search app users can access the search results)
- **Lifetime**
  - Default is 10 minutes
  - Can be extended to 7 days
  - To keep your search longer, schedule a report



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Share Search Jobs

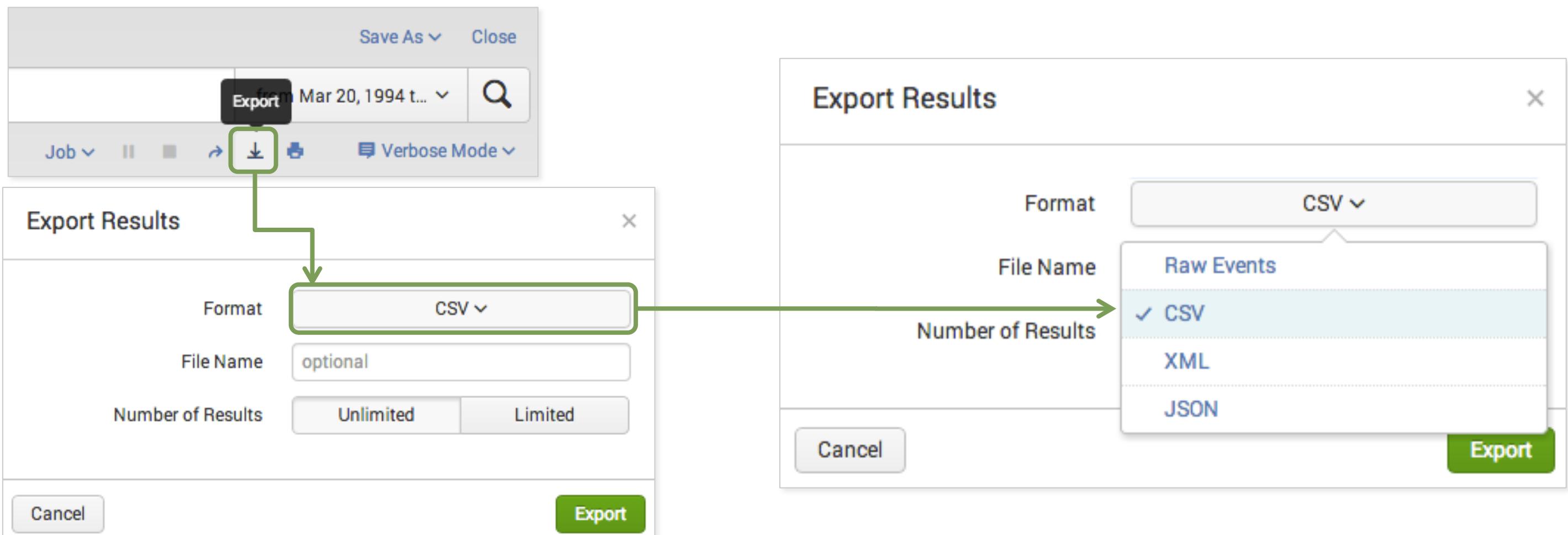
- Use the Share button next to the Job bar to quickly:
  - Apply read permissions to everyone
  - Extend the retention of the results to 7 days
  - Get a sharable link to the results
- Click the printer icon to print results or save them as PDF



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Export Search Results

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



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

The screenshot shows the Splunk web interface. At the top, there is a navigation bar with tabs for 'Messages', 'Settings', 'Activity' (which is highlighted), and 'Help'. A dropdown menu is open under 'Activity', showing options: 'Jobs' (which is also highlighted), 'Triggered Alerts', and 'System Activity'. Below this, a search bar shows the query 'from Mar 20, 1994 t...' and a magnifying glass icon.

A callout box points to the 'Activity' tab and the 'Jobs' option in the dropdown, with the text: '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)'

The main content area shows the 'Search & Reporting' search results page. The search bar at the top has 'Search & Reporting (search)' selected. Below the search bar are filters for 'Owner' (Administrator (admin)), 'Status' (All), and a search input field with a magnifying glass icon. To the right, it says '10 per page'.

The table below has columns: Dispatched at, Owner, Application, Size, Events, Run time, Expires, Status, and Actions. There are two rows of data:

Dispatched at	Owner	Application	Size	Events	Run time	Expires	Status	Actions
3/20/14 6:30:00 PM	admin	search	0.47MB	74,227	00:00:27	Saved	Done	Inspect   Delete
		"failed password"						
3/14/14 7:24:44 PM	admin	search	31.04MB	0	143:27:24	Mar 20, 2014 6:54:08 PM	Running (100%)	Inspect   Save   Pause   Finalize   Delete
		Test Login Attempts						

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

The screenshot shows the Splunk interface with the following elements:

- Top Navigation Bar:** Search, Pivot, Reports, Alerts, Dashboards, Search & Reporting.
- Search Bar:** A large input field with placeholder text "enter search here...".
- Time Filter:** A dropdown menu showing "No Time Filter" (selected), "Ran: Today", "Ran in: Last 7 Days", and "Ran in: Last 30 Days".
- Search History:** A section titled "Search History" with a "filter" button and a dropdown menu showing "No Time Filter" (selected).
- Table:** A table listing five search queries. Each row has a "Search" button and a "Last Run" timestamp. The first query is expanded to show its full text.
- Text:** A note at the bottom of the table: "Search queries are truncated to fit on a single line, but clicking the '>' icon in the leftmost column will expand long queries to display the full text."
- Callouts:**
  - Callout 1: Points to the "Search History" link in the sidebar.
  - Callout 2: Points to the "No Time Filter" dropdown menu item.
  - Callout 3: Points to the expand icon (a right-pointing arrow) in the first table row.

	Actions	Last Run
> sourcetype=cisco:asa TCP deny	Search	2 minutes ago
> sourcetype=cisco:asa NOT host=*06* ICMP   erex eid examples="302021"   rename eid as eventcode   search eventcode=10* ...	Search	3 minutes ago
> sourcetype=cisco:asa ICMP   erex eid examples="302021"   timechart count by eid	Search	3 minutes ago
> sourcetype=cisco:asa ICMP   erex eid examples="302021"	Search	3 minutes ago
> sourcetype=cisco:asa	Search	3 minutes ago

	Actions	Last Run
> sourcetype=cisco:asa TCP deny	Search	2 minutes ago
> sourcetype=cisco:asa NOT host=*06* ICMP   erex eid examples="302021"   rename eid as eventcode   search eventcode=10* ...	Search	3 minutes ago
sourcetype=cisco:asa NOT host=*06* ICMP   erex eid examples="302021"   rename eid as eventcode   search eventcode=10* NOT isnull(sourceip)   fields eventcode_time   bucket_time span=60m   timechart count by eid limit=10		
> sourcetype=cisco:asa ICMP   erex eid examples="302021"   timechart count by eid	Search	3 minutes ago
> sourcetype=cisco:asa ICMP   erex eid examples="302021"	Search	3 minutes ago
> sourcetype=cisco:asa	Search	3 minutes ago

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Using Fields in Searches

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

The image shows four separate search boxes, each with a search bar, a time range selector (All time), and a magnifying glass icon. The search terms are:

- area\_code=404
- action=purchase status=503
- source=/var/log/messages\* NOT host=mail12
- sourcetype=access\_combined

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

< Hide Fields		All Fields	I	Time	Event
			>	9/8/14 9:09:53.000 PM	174.123.217.162 - - [08/Sep/2014:21:09:53] "POST /cart/success.do?JSESS IONID=SD2SL7FF3ADFF4956 HTTP 1.1" 200 2123 "http://www.buttercupgames.com /cart.do?action=purchase&itemId=EST-18" "Mozilla/5.0 (Macintosh; Intel M ac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.4 6 Safari/536.5" 854  action = purchase   host = www3   source = /opt/log/www3/access.log   sourcetype = access_combined   status = 200
			>	9/8/14 9:09:53.000 PM	174.123.217.162 - - [08/Sep/2014:21:09:53] "POST /cart.do?action=purchas e&itemId=EST-18&JSESSIONID=SD2SL7FF3ADFF4956 HTTP 1.1" 200 548 "http://w ww.buttercupgames.com/cart.do?action=addtocart&itemId=EST-18&categoryI=

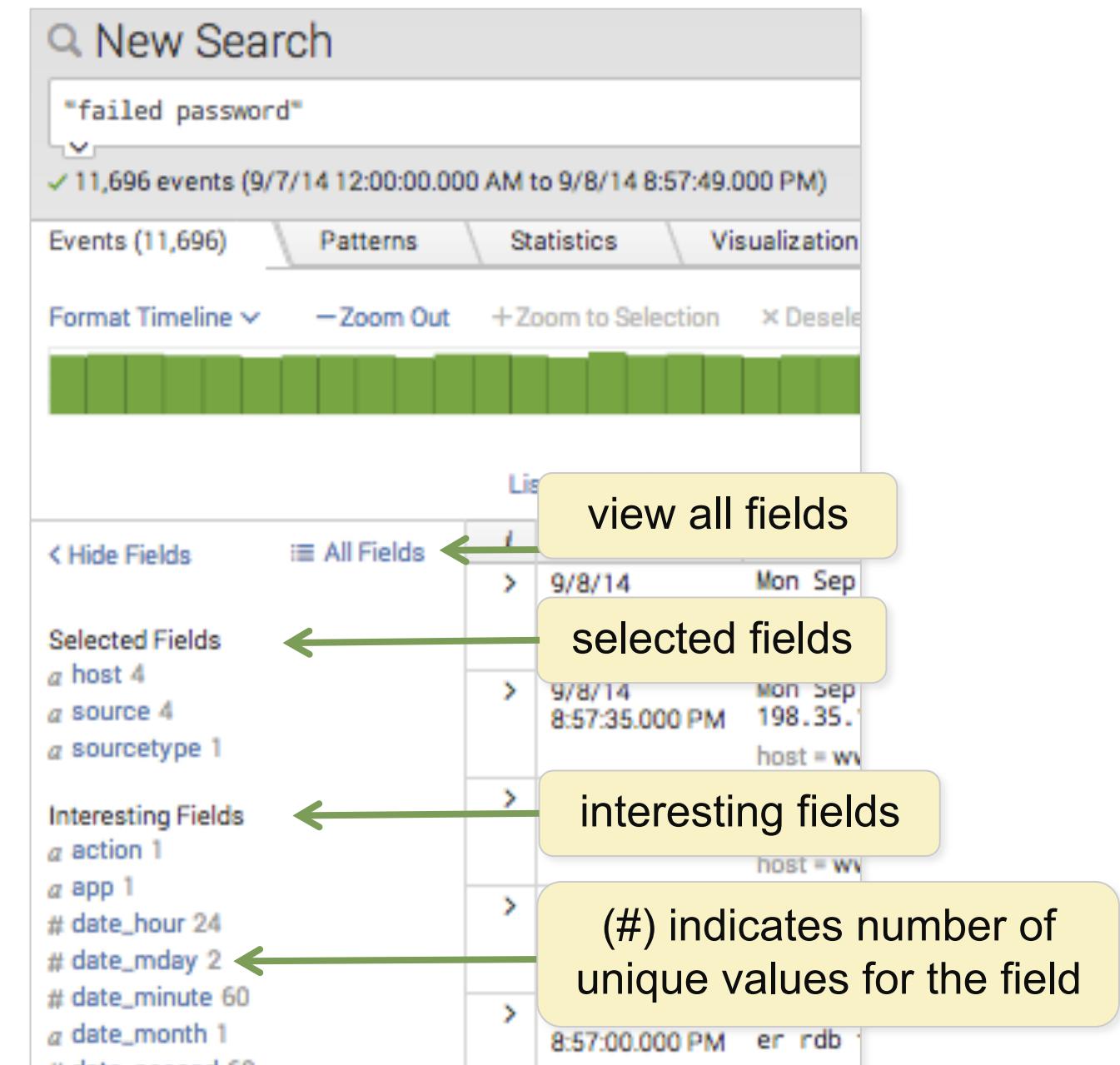
- Sometimes not (e.g., status=302)

< Hide Fields		All Fields	I	Time	Event
			>	9/8/14 5:49:33.805 PM	1410198573.805 223 207.36.232.245 TCP_MISS/302 679 GET http://www.glob alhealthreporting.org/ lsagers@buttercupgames.com DIRECT/www.globalhealt hreporting.org text/html DEFAULT_CASE-DefaultGroup-Demo_Clients-NONE-NO NE-DefaultRouting <Iw_news,5.0,0,-,-,-,0,-,-,-,-,-,Iw_news,-> -- action = TCP_MISS   host = cisco_router1   source = /opt/log/cisco_router1/cisco_ironport_web.log   sourcetype = cisco_wsa_squid   status = 302
			>	9/8/14	1410167891.061 993 27.96.191.11 TCP_MISS/302 256 GET http://www.dyson.c om/... DIRECT/www.dyson.com DEFAULT_CASE-Def

- For more information, please see: <http://docs.splunk.com/Documentation/Splunk/latest/Data>Listofpretrainedsourcetypes>  
Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Use Fields in Searches

- Efficient way to pinpoint searches and refine results



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

Three search boxes are shown, each with a different case for the field name:

- host=www3 (323 events)
- host=WWW3 (323 events)
- HOST=www3 (0 events)

These two searches return results

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)

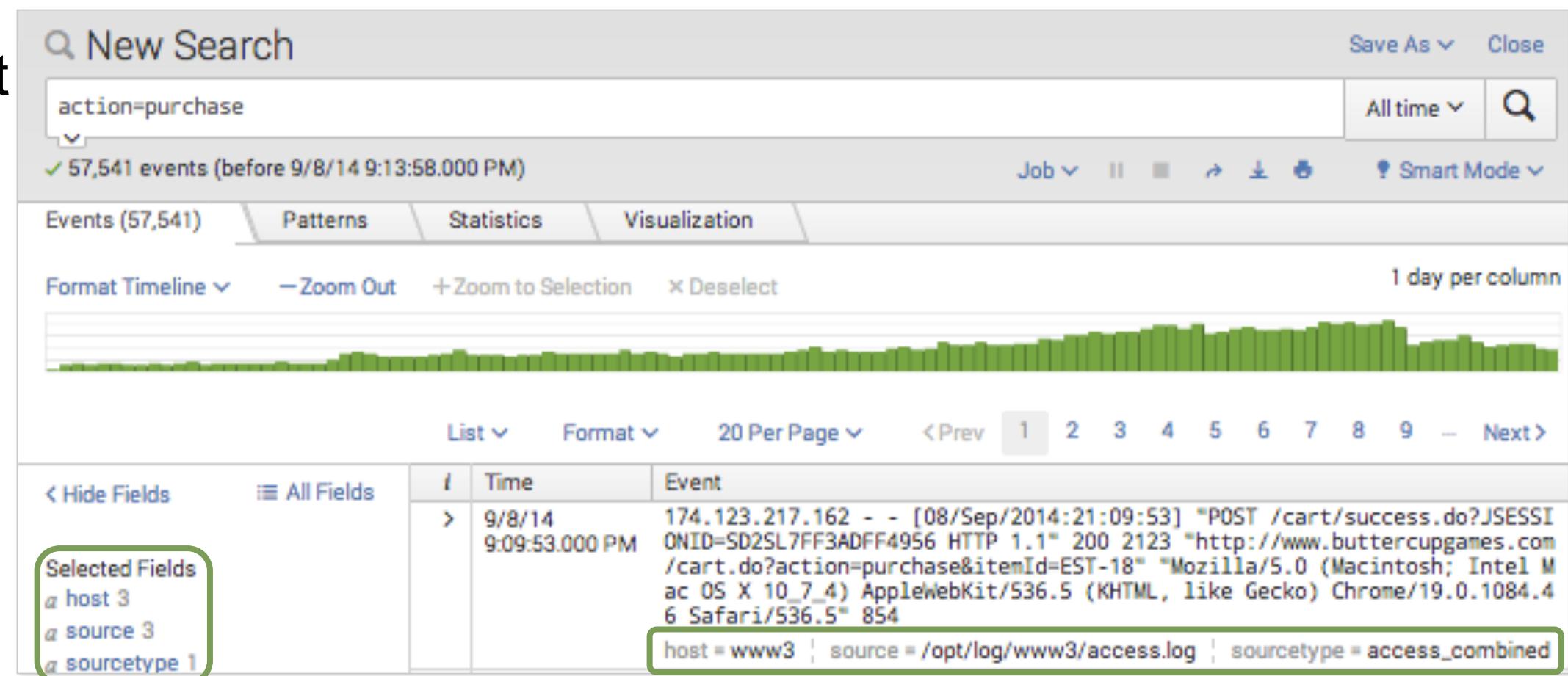
```
user=* sourcetype=access* (referer_domain=*.cn OR referer_domain=*.hk)
```

- 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.



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Make an Interesting Field Selected

You can modify selected fields

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

The screenshot shows the Splunk interface with two main windows. The top window is a 'Selected Fields' dialog, and the bottom window is a search results page.

In the 'Selected Fields' dialog (top left), there is a sidebar titled 'Selected Fields' containing 'host 3', 'source 3', and 'sourcetype 1'. Below this is a list titled 'Interesting Fields' with 'action 1' highlighted by a green box and circled with a red number '1'. To the right of the dialog is a search results table for the event 'ONID=SD2SL7FF3ADFF4956 HTTP 1.1" 200 2123 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-18" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_7\_4) AppleWebKit/536.5 (KHTML, like Gecko) Safari/536.5" 854'. The 'action' field is listed under 'Selected Fields' in the table header. The 'action' column has a value of 'purchase' with a count of 57,541 and 100% frequency. A 'Selected' checkbox is checked and circled with a red number '2', with 'Yes' selected.

The bottom window shows a search for 'action=purchase' with 57,541 events found. The results table has columns for Time and Event. The first event listed is from 9/8/14 at 9:09:53.000 PM with the event details: '174.123.217.162 - - [08/Sep/2014:21:09:53] "POS ONID=SD2SL7FF3ADFF4956 HTTP 1.1" 200 2123 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-18" "Mozilla/5.0 (Mac OS X 10\_7\_4) AppleWebKit/536.5 (KHTML, like Gecko) Safari/536.5" 854'. The 'action' field is also listed under 'Selected Fields' in the table header.

Now that it is a selected field, it appears

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

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Make Any Field Selected

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

The screenshot shows the Splunk interface with the 'Select Fields' modal open. The modal has a header 'Select Fields' with buttons for 'Select All Within Filter', 'Deselect All', 'Coverage: 1% or more', and a 'filter' search bar. The main table lists fields with columns for checked status, field name, # of Values, Event Coverage, and Type. A green arrow points from the 'All Fields' button in the sidebar to the 'action' field in the table.

	Field	# of Values	Event Coverage	Type
<input checked="" type="checkbox"/>	host	8	100%	String
<input checked="" type="checkbox"/>	index	1	100%	String
<input checked="" type="checkbox"/>	linecount	5	100%	Number
<input checked="" type="checkbox"/>	price	7	10.9%	Number
<input checked="" type="checkbox"/>	source	13	100%	String
<input checked="" type="checkbox"/>	sourcetype	9	100%	String
<input checked="" type="checkbox"/>	splunk_server	1	100%	String
<input type="checkbox"/>	AcctID	15	3.99%	String
<input type="checkbox"/>	Address	1	1.06%	String
<input type="checkbox"/>	Address_Description	2	1.06%	String
<input type="checkbox"/>	Clock	1	1.06%	String
<input type="checkbox"/>	Code	9	3.99%	String

**All Fields** (7 Values, 63.323%)

**Selected Fields**

- a host 1
- a index 1
- # linecount 1
- # price 7
- a source 2
- a sourcetype 2
- a splunk\_server 1

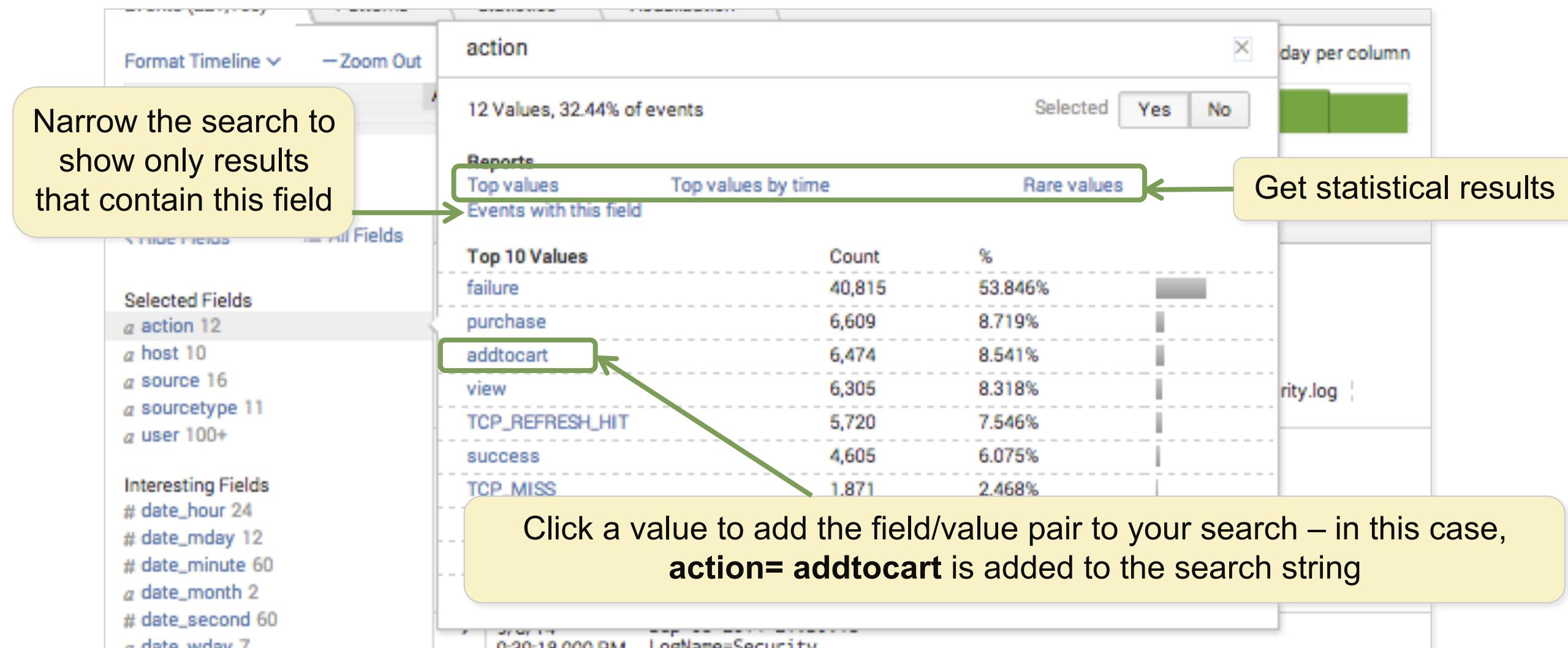
**Interesting Fields**

- a action 7
- a app 2
- # bytes 100+
- a categoryid 8
- a clientip 73

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# The Field Window

Select a field from the fields sidebar, then:



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

The screenshot shows the Splunk search interface with a search query "host=www3" and a result count of 182,857 events. A context menu is open over the "Fast Mode" button in the top right, listing three options: Fast Mode (selected), Smart Mode, and Verbose Mode.

**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.

Time	Event
9/8/14 10:15:17.000 PM	Mon Sep 08 2014 22:15:17 www3 sshd[1118]: Failed password for invalid user henri from 10.3.10.46 port 4095 ssh2 host = www3   source = /opt/log/www3/secure.log   sourcetype = linux_secure
9/8/14 10:15:07.000 PM	Mon Sep 08 2014 22:15:07 www3 sshd[1953]: Failed password for invalid user sapadmin from 10.3.10.46 port 2172 ssh2 host = www3   source = /opt/log/www3/secure.log   sourcetype = linux_secure
9/8/14 10:14:51.000 PM	Mon Sep 08 2014 22:14:51 www3 sshd[5007]: Failed password for invalid user edmond from 10.3.10.46 port 4292 ssh2 host = www3   source = /opt/log/www3/secure.log   sourcetype = linux_secure
9/8/14	Mon Sep 08 2014 22:14:39 www3 sshd[44370]: Accepted password for djohnson from 10.3.10.46 port 1591 ssh2

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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 • Yes	• 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

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Creating Reports and Visualizations

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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>

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Create a Report from Search

- 1 Run a search
- 2 Select Save As
- 3 Select Report

The screenshot shows the Splunk interface with the following steps highlighted:

- 1 Run a search: A search bar at the top contains the query `sourcetype=access_combined action=purchase status!=200`. A red circle with '1' indicates this step.
- 2 Select Save As: A context menu is open on the right side, with the 'Report' option highlighted by a red circle with '2'.
- 3 Select Report: The 'Report' option in the context menu is selected, indicated by a red circle with '3'.

The main search results table displays two events:

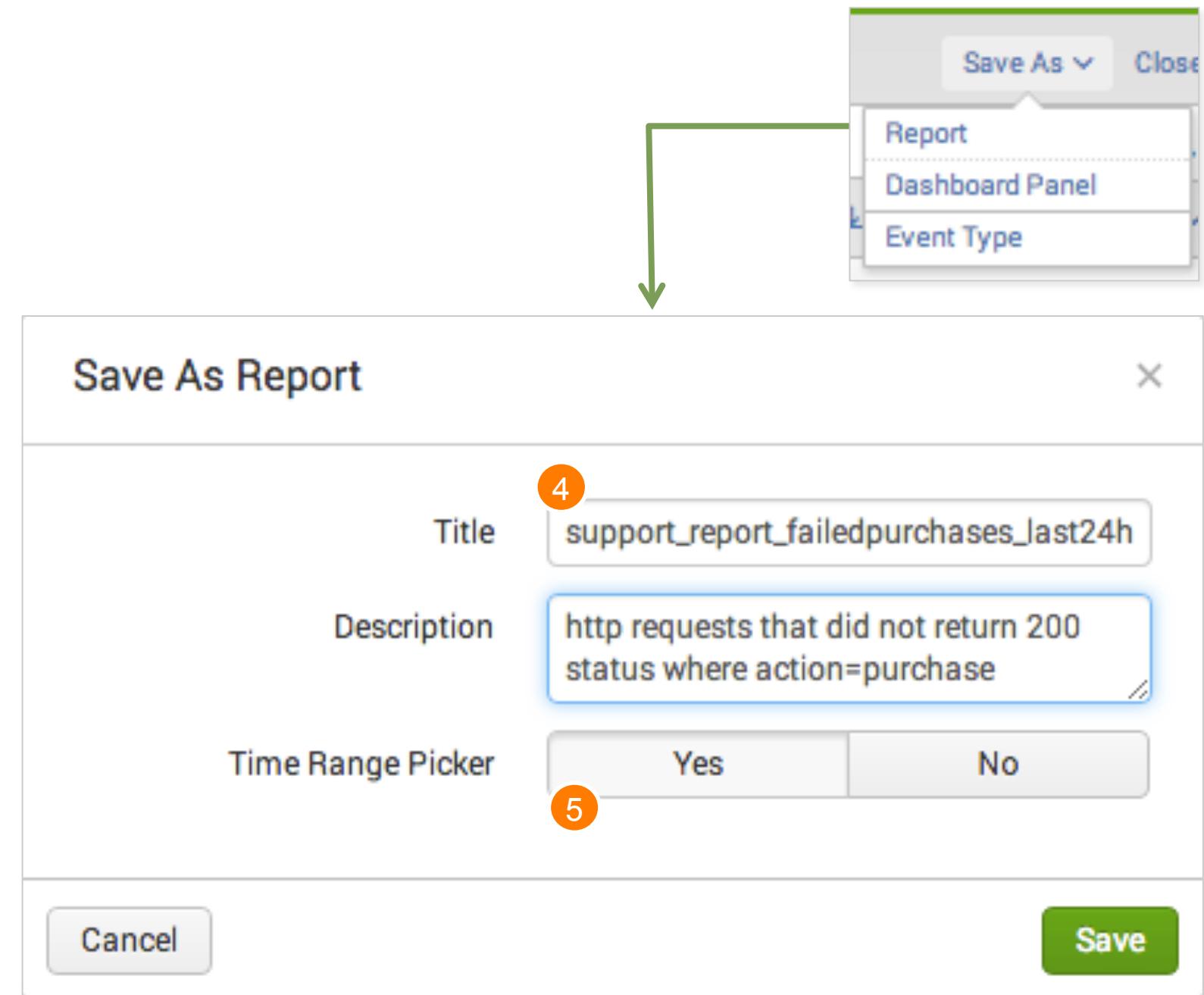
I	Time	Event
>	9/8/14 9:17:25.000 PM	175.44.1.122 - - [08/Sep/2014:21:17:25] "POST /cart.do?action=purchase&itemId=EST-13&JSESSIONID=SD5SSL6FF7ADFF4954 HTTP/1.1" 503 2166 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-13&categoryId=STRATEGY&productId=DC-SG-G02" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 983 action = purchase   host = www3   source = /opt/log/www3/access.log   sourcetype = access_combined   user = -
>	9/8/14 8:52:33.000 PM	125.7.55.180 - - [08/Sep/2014:20:52:33] "POST /cart.do?action=purchase&itemId=EST-17&JSESSIONID=SD2SL1FF6ADFF4955 HTTP/1.1" 503 3897 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-17&categoryId=ACCESSORIES&productId=WCSH-A02" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)" 999 action = purchase   host = www1   source = /opt/log/www1/access.log   sourcetype = access_combined   user = -

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

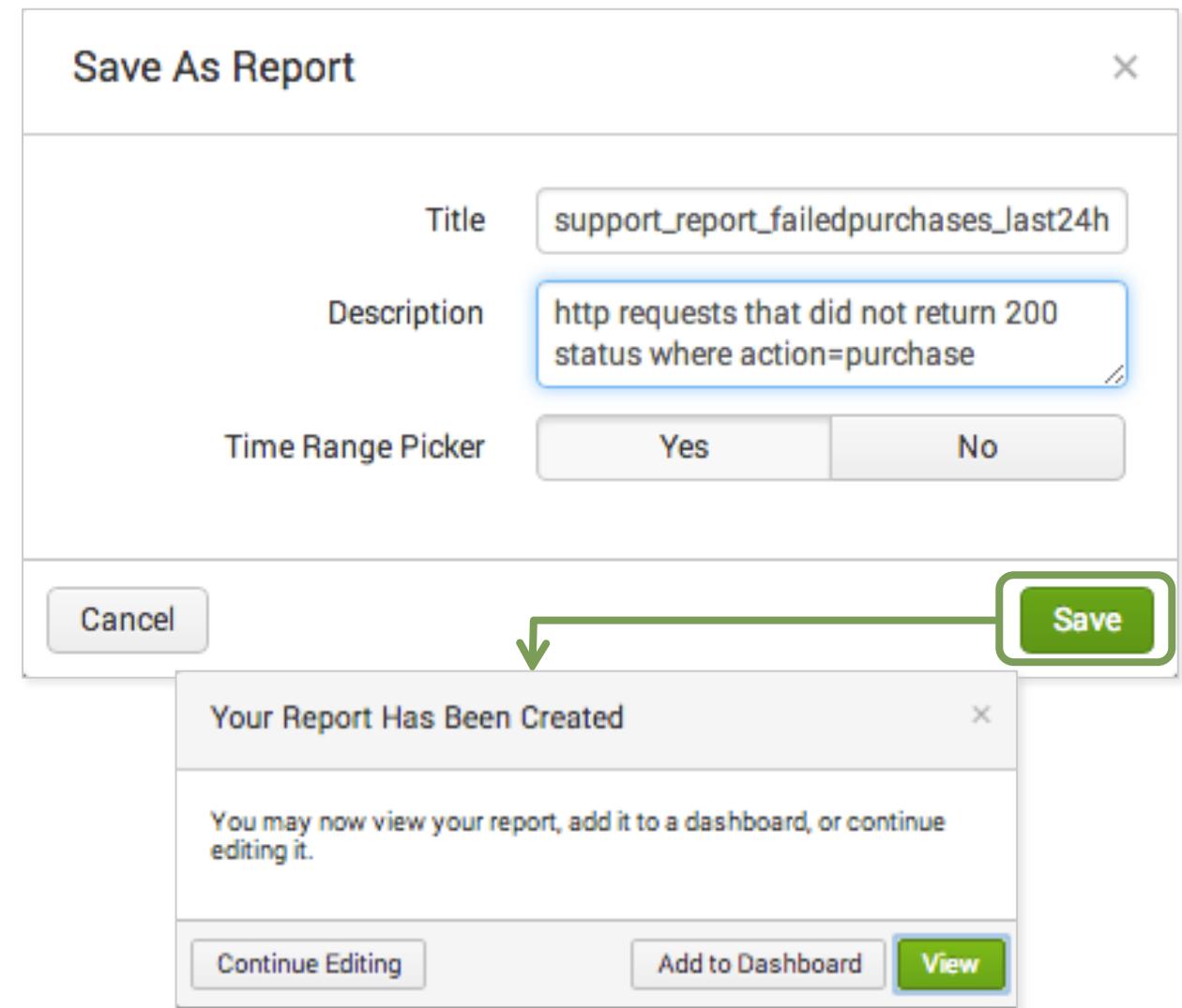


Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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)

The screenshot shows the Splunk web interface. On the left, there's a sidebar with 'Search', 'Pivot', 'Reports' (which is selected and highlighted in green), 'Alerts', and 'Dashboards'. Below this, under 'Reports', there's a heading 'Reports' and a sub-section '5 Reports' with buttons for 'All', 'Yours', 'This App's', and 'Filter'. A green arrow points from the 'Reports' button in the sidebar to the 'support\_report\_failed\_purchases...' report in the list. The main content area has a green header bar with 'Search', 'Pivot', 'Reports', 'Alerts', 'Dashboards', and 'Search & Reporting'. Below this is a search bar containing the report title 'support\_report\_failed\_purchases\_last\_30\_days'. To the right of the search bar are 'Edit', 'More Info', and 'Add to Dashboard' buttons. A green box highlights the 'Last 30 days' dropdown menu. Below the search bar, the text '1,837 events (8/9/14 12:00:00.000 AM to 9/8/14 9:42:24.000 PM)' is displayed. Further down, there's a table with columns 'Time' and 'Event', showing two log entries. The first entry is from '9/8/14 9:17:25.000 PM' and the second is from '9/8/14 8:52:33.000 PM'.

Time	Event
9/8/14 9:17:25.000 PM	175.44.1.122 - - [08/Sep/2014:21:17:25] "POST /cart.do?action=purchase&itemId=EST-13&JSESSIONID=SD5SL6F F7ADFF4954 HTTP/1.1" 503 2166 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-13&category=STRATEGY&productId=DC-SG-G02" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 983 action = purchase   host = www3   source = /opt/log/www3/access.log   sourcetype = access_combined   user = -
9/8/14 8:52:33.000 PM	125.7.55.180 - - [08/Sep/2014:20:52:33] "POST /cart.do?action=purchase&itemId=EST-17&JSESSIONID=SD2SL1F F6ADFF4955 HTTP/1.1" 503 3897 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-17&category=ACCESSORIES&productId=WC-SH-A02" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)" 999

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

The screenshot shows a Splunk search interface for a report titled "support\_report\_failedpurchases\_last24h". The search query is "sourcetype=access\_combined action=purchase status!=200". The results show 13 of 311 events matched. The interface includes a timeline, event list, and various navigation and configuration buttons. A context menu is open over the search bar, listing options: Edit, More Info, Add to Dashboard, Open in Search, Edit Description, Edit Permissions, Edit Acceleration, Clone, and Delete.

support\_report\_failedpurchases\_last24h

sourcetype=access\_combined action=purchase status!=200

13 of 311 events matched

Events (13) Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

24 hour window ▾ 13 of 311 events matched 20 per page ▾

Time Event

i	Time	Event
>	3/20/14 8:55:20.000 PM	94.229.0.20 - - [20/Mar/2014:20:55:20] "POST /cart.do?action=D=SD85L10FF3ADFF4960 HTTP/1.1" 503 968 "http://www.buttercupgolf.com/EST-19&category=SPORTS&productId=CU-PG-G06" "Mozilla/5.0 (Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1.26
		host = www2 dmz team web   index = main   linecount = 1   price = 19.99   source = /opt/log/www2/access.log   sourcetype = access_combined   split
		SESSIONID=SD85L10FF3ADFF4960 HTTP/1.1" 503 968 "http://www.buttercupgolf.com/EST-19&category=SPORTS&productId=CU-PG-G06" "Mozilla/5.0 (Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1.26
		Mobile/9B206 Safari/7534.48.3" 926
		access.log   sourcetype = access_combined
		SESSIONID=SD85L10FF3ADFF4960 HTTP/1.1" 503 968 "http://www.buttercupgolf.com/EST-19&category=SPORTS&productId=CU-PG-G06" "Mozilla/5.0 (Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1.26
		Mobile/9B206 Safari/7534.48.3" 926
		access.log   sourcetype = access_combined
		SESSIONID=SD85L10FF3ADFF4960 HTTP/1.1" 503 968 "http://www.buttercupgolf.com/EST-19&category=SPORTS&productId=CU-PG-G06" "Mozilla/5.0 (Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1.26
		Mobile/9B206 Safari/7534.48.3" 926
		access.log   sourcetype = access_combined

Generated for James Kim (455-641720) (C) Splunk Inc. not for distribution

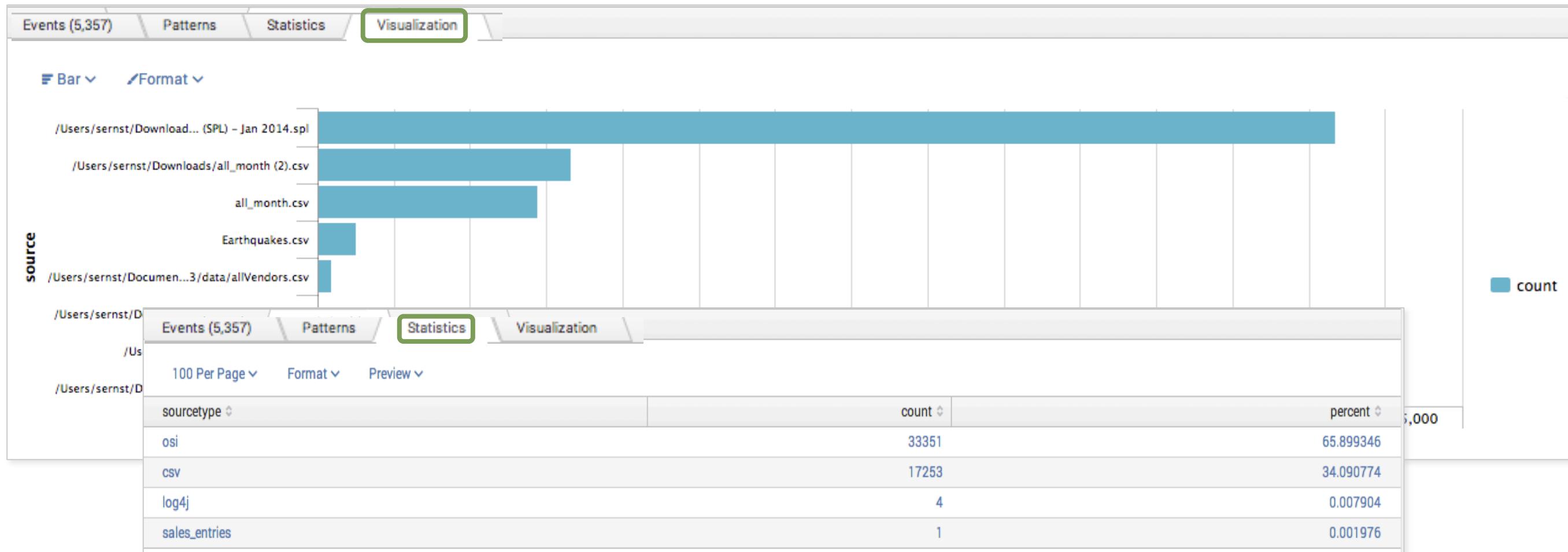
# Create Tables and Visualizations

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

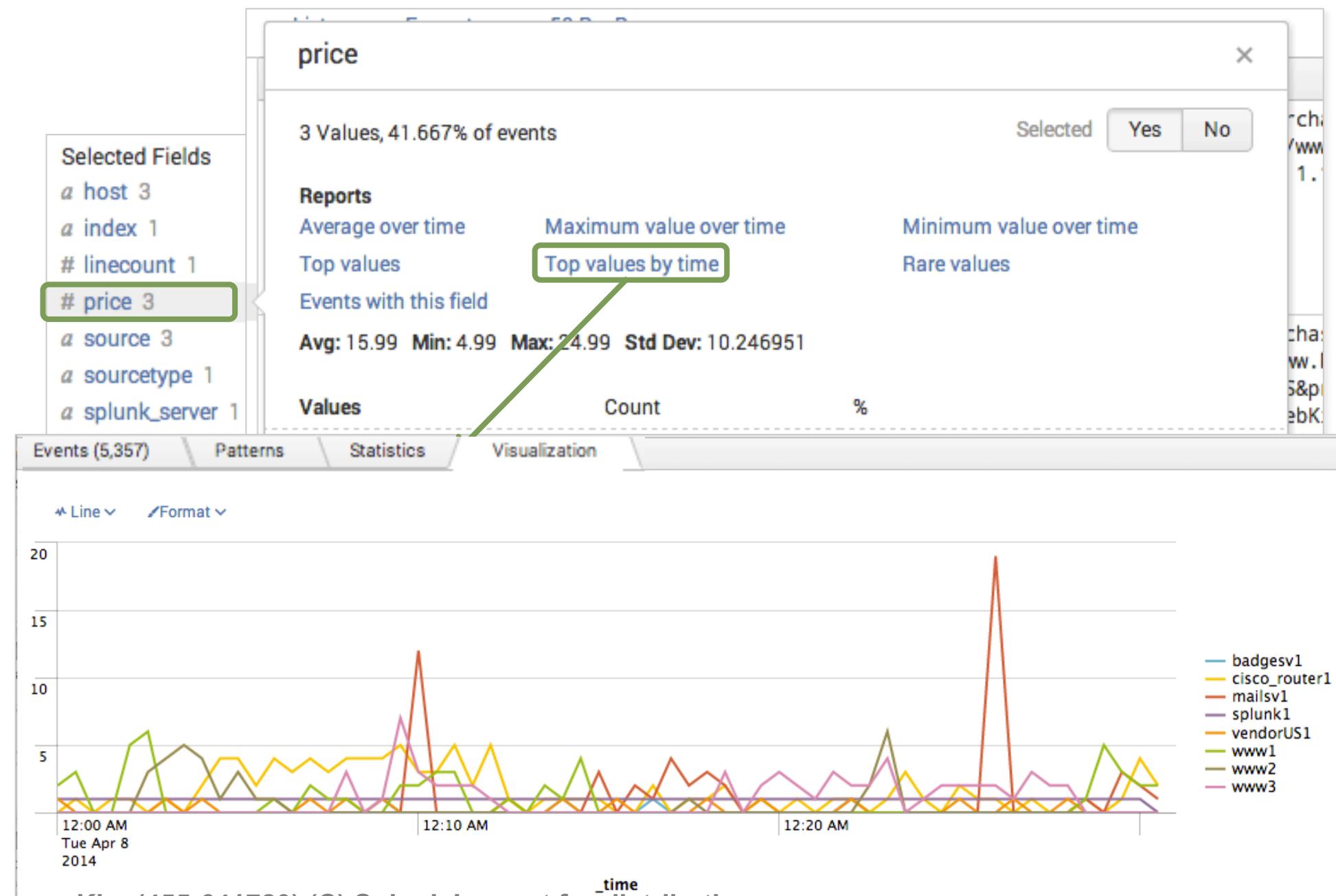
- Statistical reports leverage Splunk's built-in visualizations or table format
- These views give you insights into your organization's data



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Create Reports From the Field Window

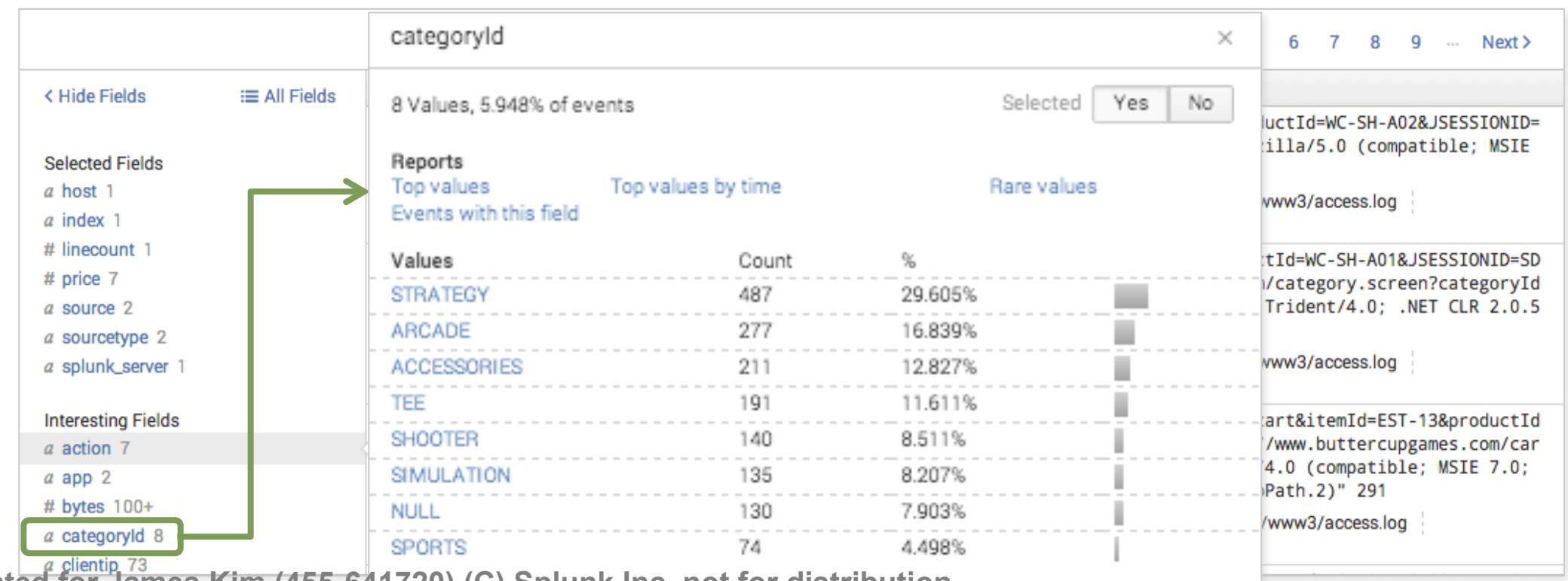
- For numeric fields, you can create reports with mathematical functions such as average, maximum value, and minimum value
- In this example, it generates a report that shows top values by time
  - This is known as a timechart



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Create a Top Values Report

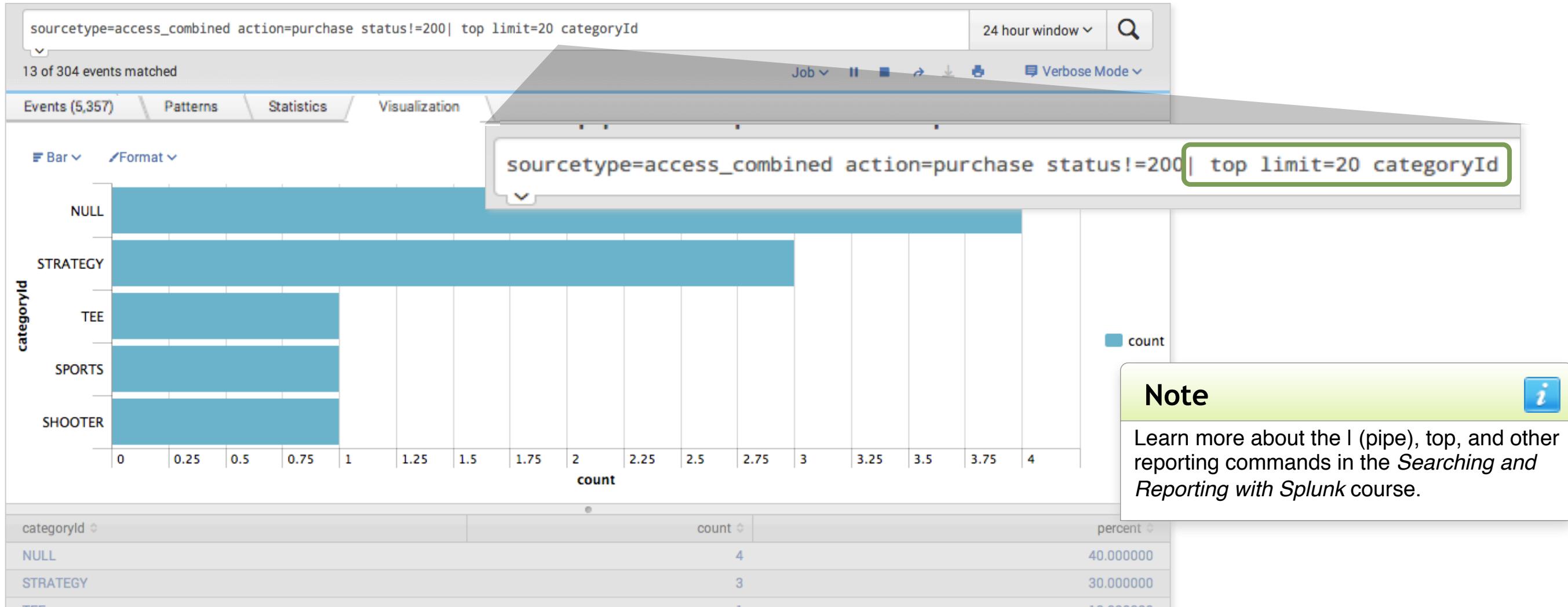
- For character fields, there are only 3 available reports
- We want a report that show us the top **categories** purchased
  - Example search: sourcetype=access\_combined status=200 action=purchase
  - Click the **categoryId** field
  - Click **Top values**



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Create a Top Values Report (cont.)

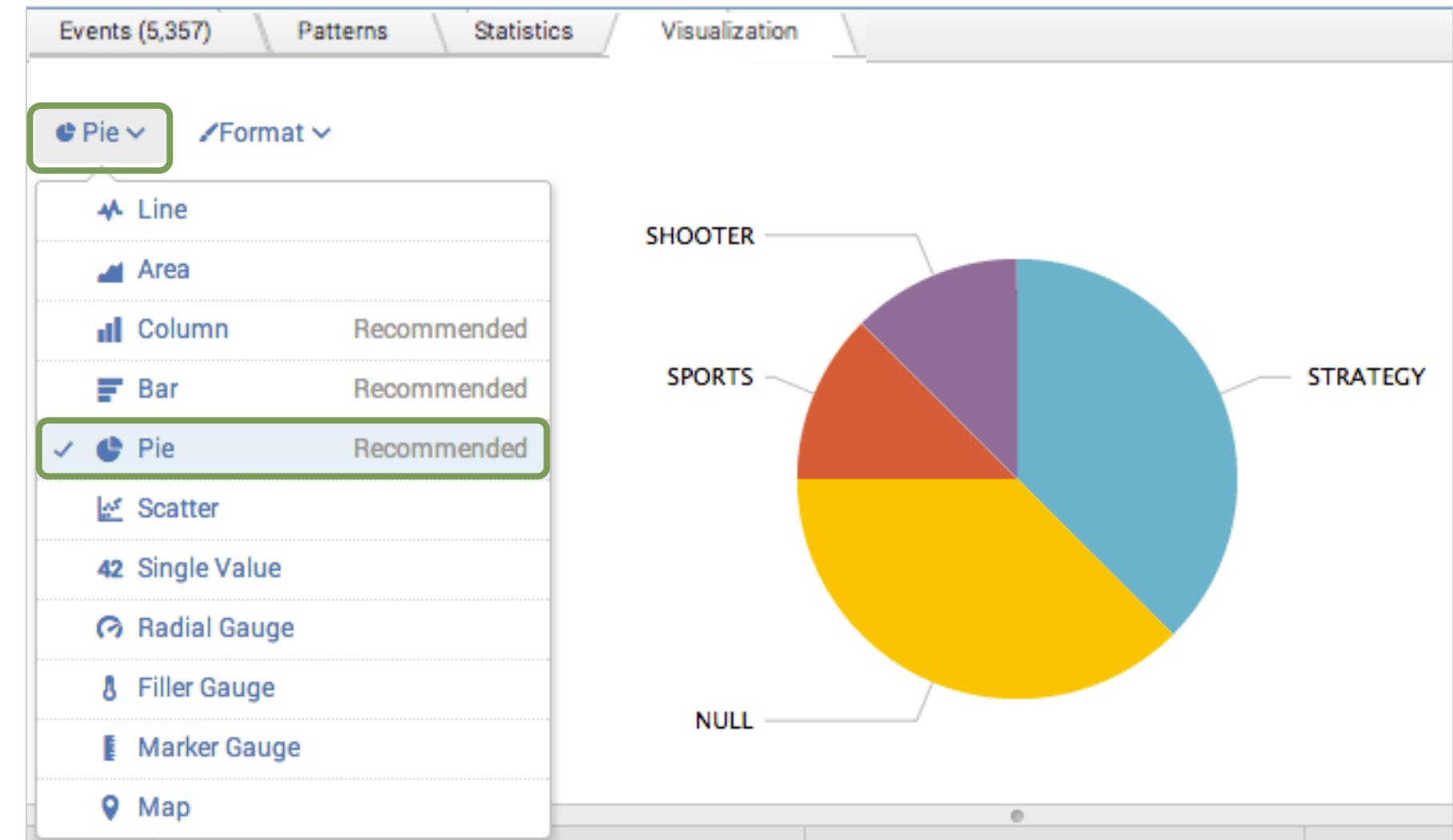
A | (pipe) and the top command is added to the search string and returns a bar chart on the Visualizations tab of the top categories purchased



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Change the Visualization

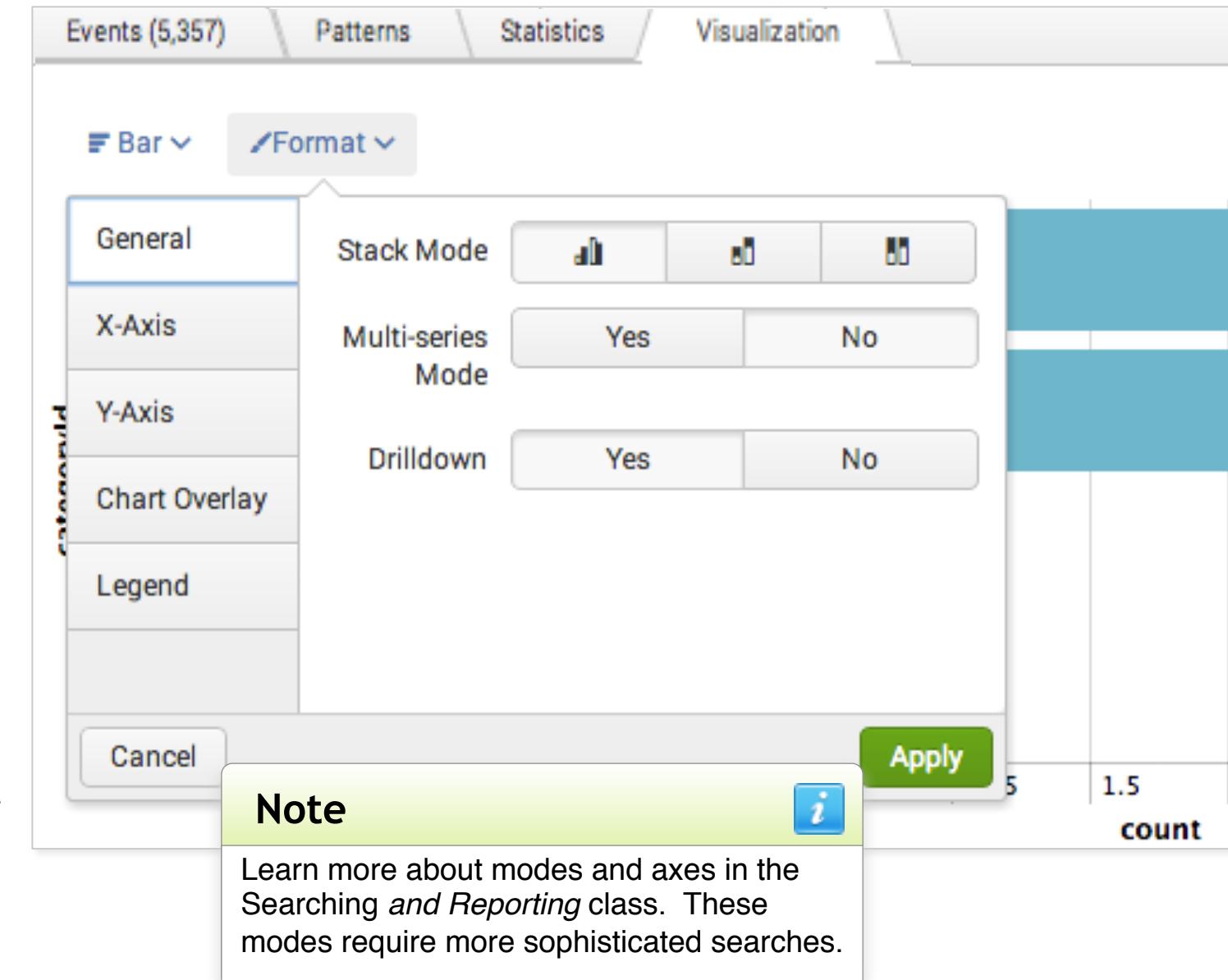
- Select a visualization from the **Type** dropdown menu
- In this example, the bar chart is changed to a pie chart



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# View as a Table

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

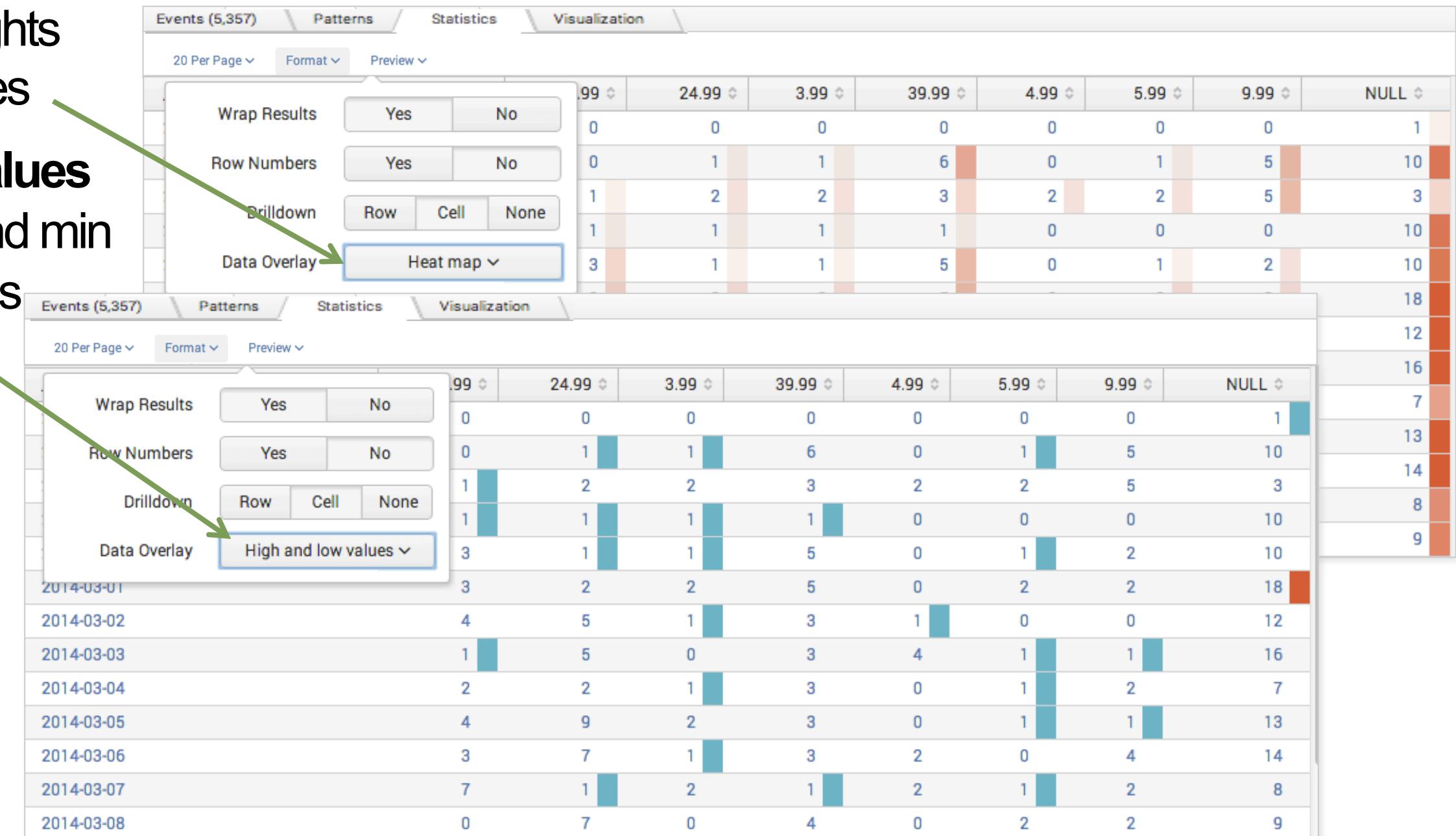
The screenshot shows the Splunk interface with the Statistics tab selected. The top navigation bar includes tabs for Events (5,357), Patterns, Statistics, and Visualization. Below the navigation bar, there are dropdown menus for 10 Per Page, Format, and Preview. The main content area is a table with the following data:

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

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Statistics Overlays

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



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Using Pivot

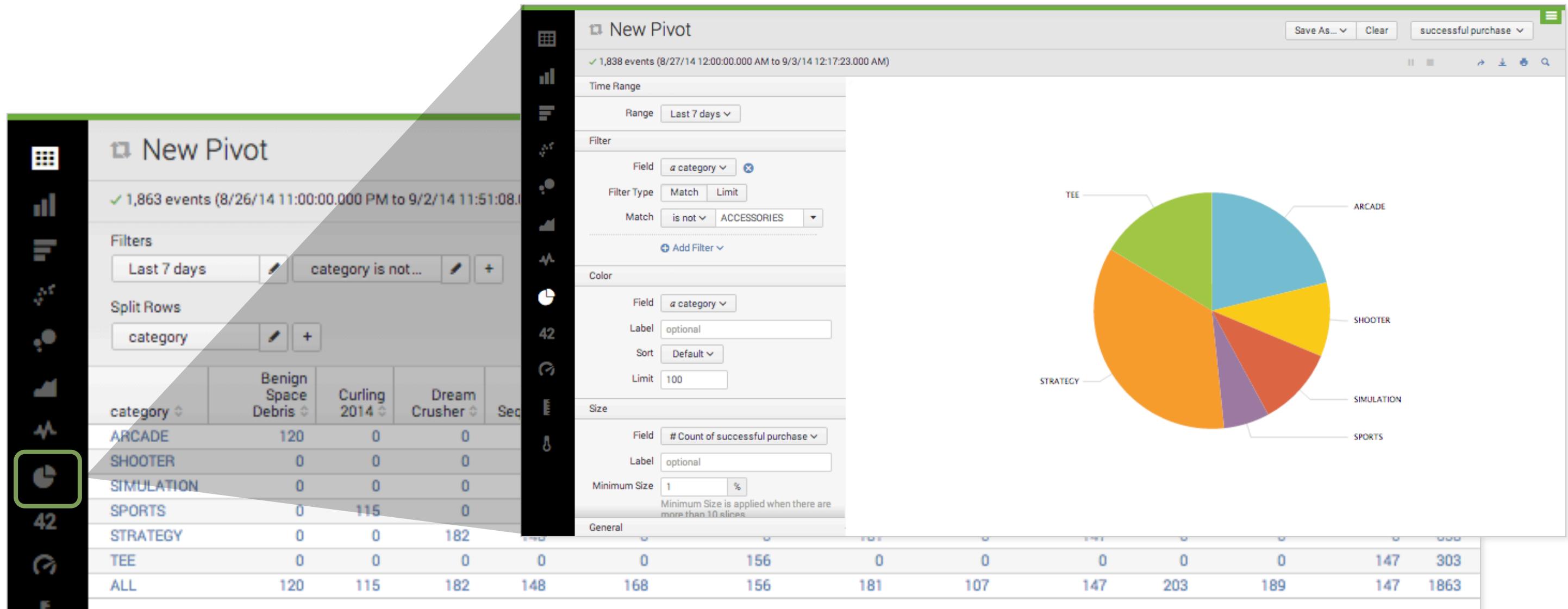
Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

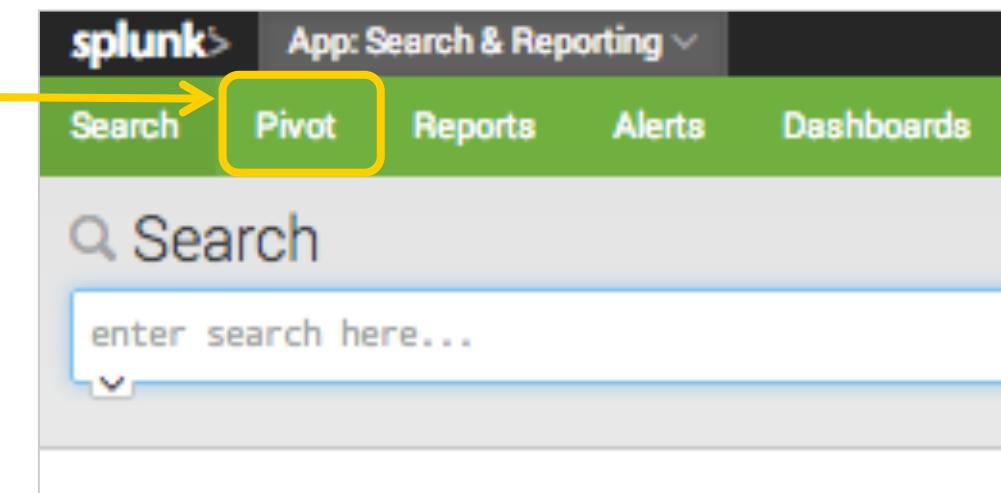
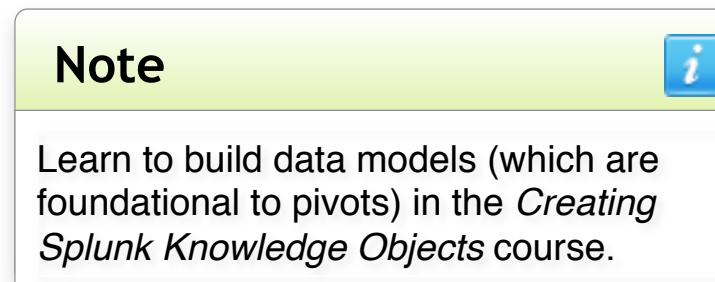
Pivot is a quick way to design visualizations of data. Let's see how.



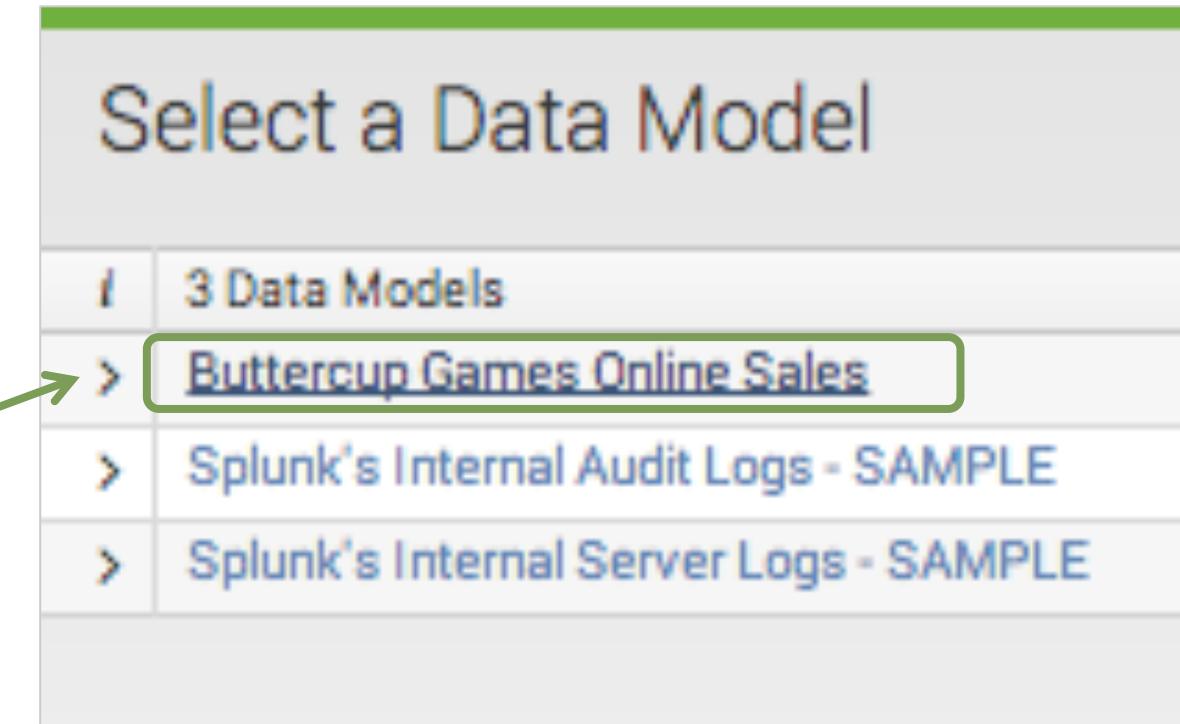
Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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



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



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

Select a Data Object  
[< Back](#)

<a href="#">i</a>	<a href="#">9 Objects in Buttercup Games Online Sales</a>
<a href="#">&gt;</a>	<a href="#">http request</a>
<a href="#">&gt;</a>	<a href="#">successful request</a>
<a href="#">&gt;</a>	<a href="#">successful purchase</a>
<a href="#">&gt;</a>	<a href="#">successful add to cart</a>
<a href="#">&gt;</a>	<a href="#">successful remove</a>
<a href="#">&gt;</a>	<a href="#">failed request</a>
<a href="#">&gt;</a>	<a href="#">failed purchase</a>
<a href="#">&gt;</a>	<a href="#">failed add to cart</a>
<a href="#">&gt;</a>	<a href="#">failed remove</a>

Click **an object** to display the count of events that you can report on

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

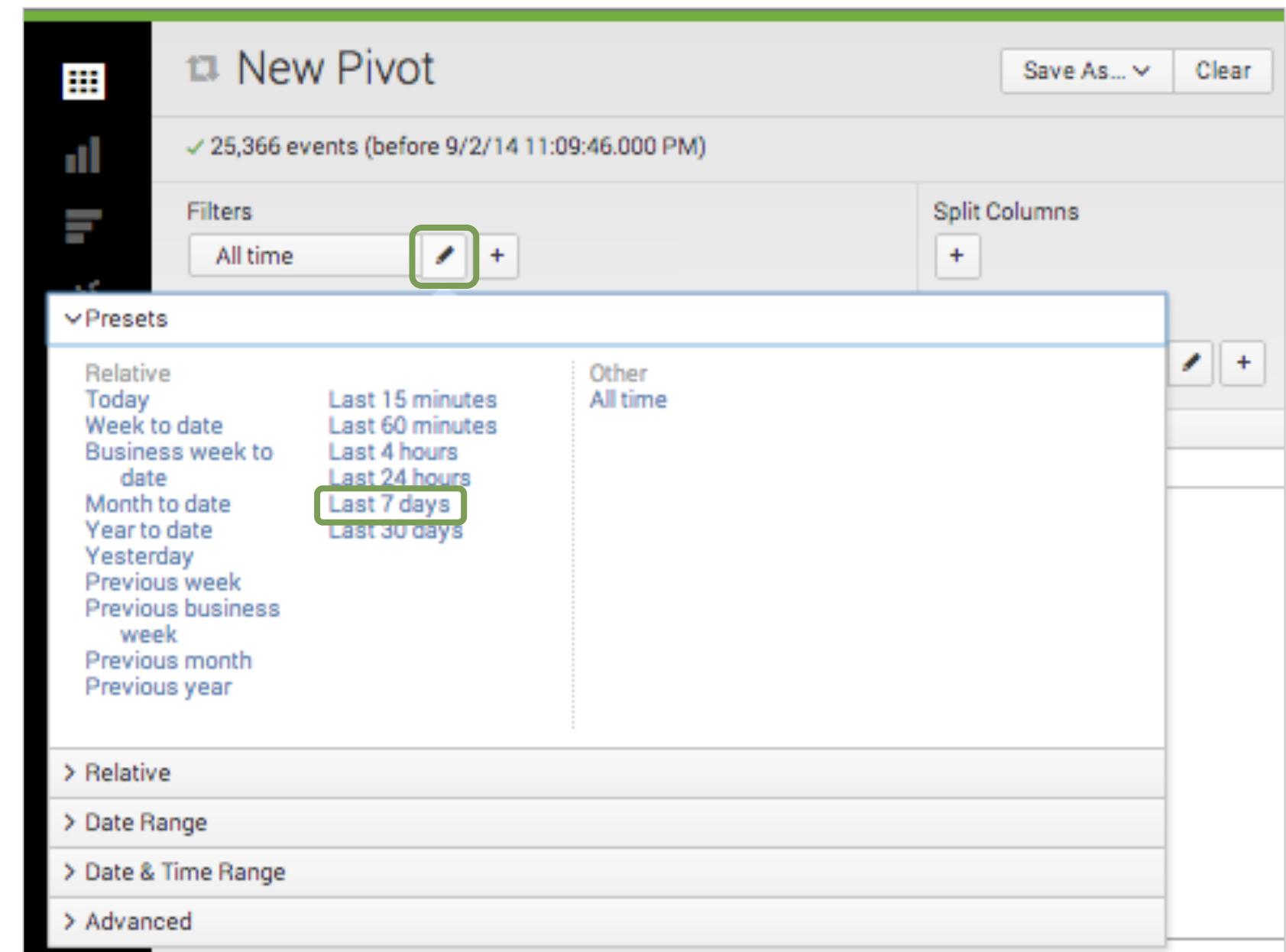
The screenshot shows the Splunk Pivot interface with the following details:

- Title Bar:** "New Pivot" with a save button, clear button, and a dropdown set to "successful purchase".
- Event Count:** "25,366 events (before 9/2/14 11:09:46.000 PM)"
- Filters:** "All time" with edit and add buttons.
- Split Rows:** An empty row with an add button.
- Column Values:** A section containing a "Count of successful purchase" field with the value "25366". This field is highlighted with a green rounded rectangle.
- Split Columns:** An empty column with an add button.
- Documentation:** A link labeled "Documentation" with a help icon.

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Select a Time Range

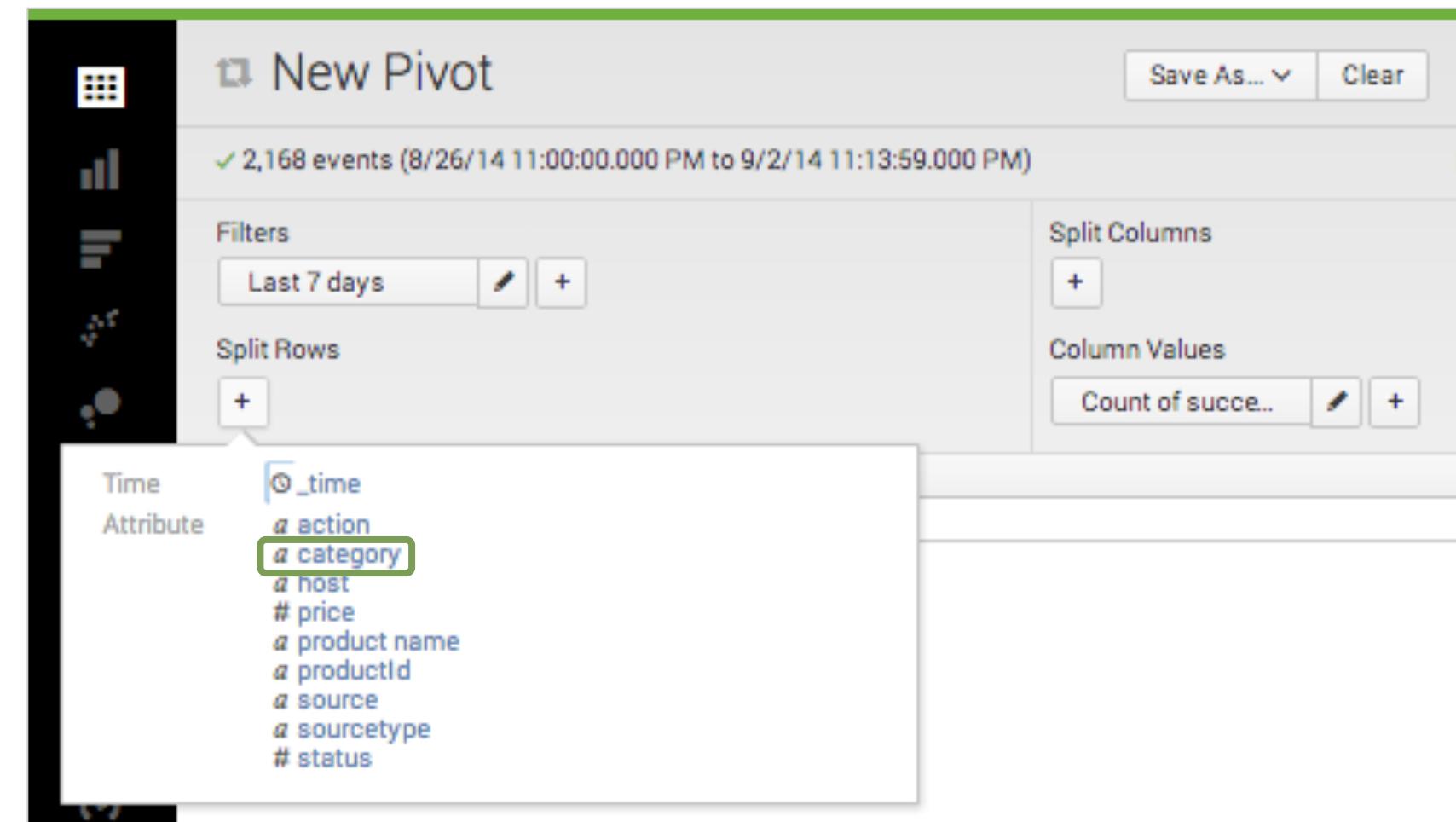
- The default is **All Time**
- Click the pencil icon to select the desired time range
- The pivot runs immediately upon selecting the new time range



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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



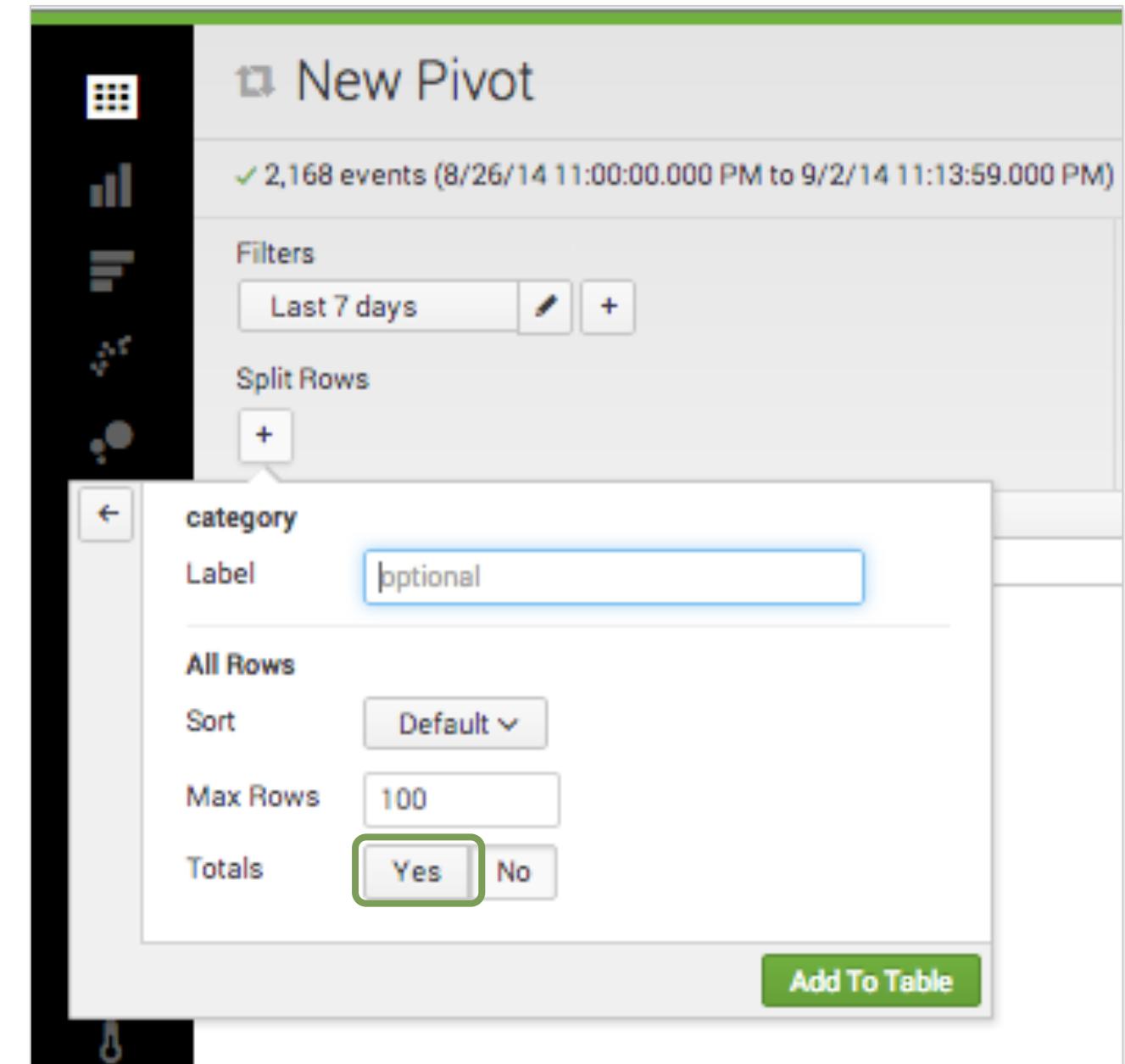
The screenshot shows the Splunk Pivot interface with the following configuration:

- Filters:** Last 7 days
- Split Rows:** A dropdown menu is open, showing a list of available fields:
  - Time
  - Attribute
  - \_time
  - ¤ action
  - ¤ category** (highlighted with a green box)
  - ¤ host
  - # price
  - ¤ product name
  - ¤ productId
  - ¤ source
  - ¤ sourcetype
  - # status
- Column Values:** Count of succe...

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Results

New Pivot

Save As... Clear successful purchase

✓ 2,168 events (8/26/14 11:00:00.000 PM to 9/2/14 11:23:39.000 PM)

Filters Last 7 days Split Columns Documentation

Split Rows category Column Values

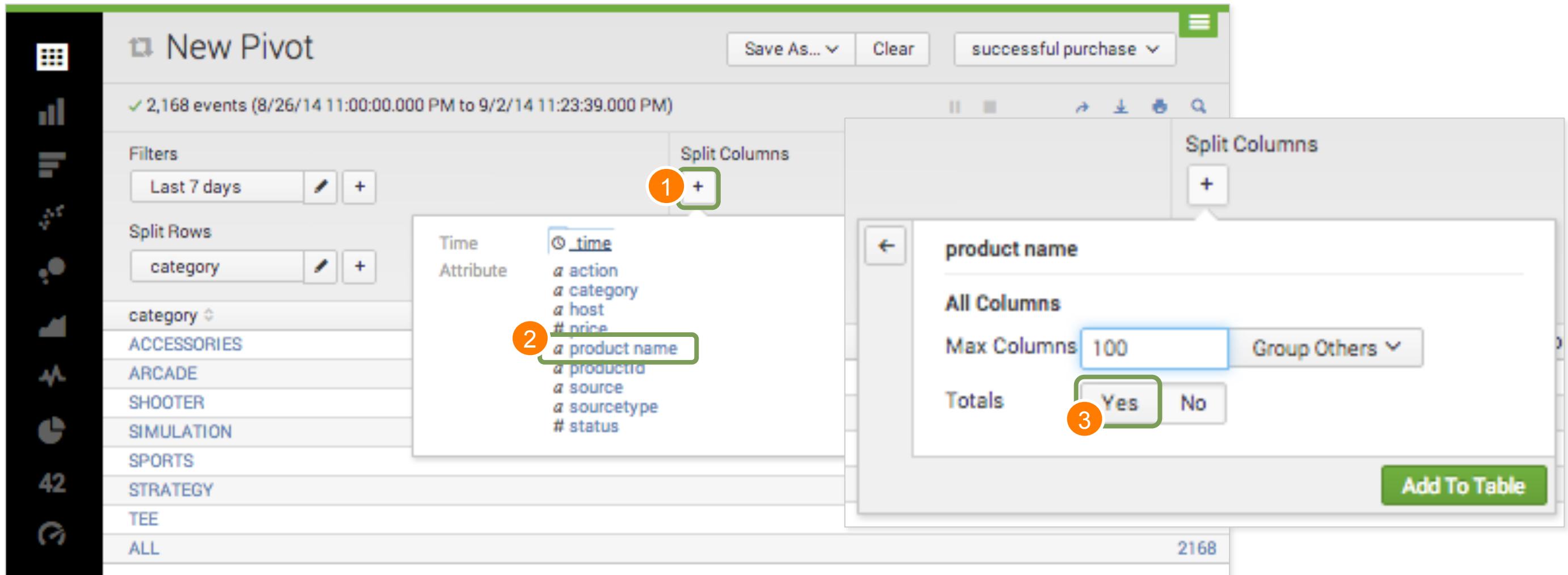
category	Count of successful purchase
ACCESSORIES	312
ARCADE	395
SHOOTER	188
SIMULATION	202
SPORTS	115
STRATEGY	656
TEE	300
ALL	2168

Categories Total Count by category

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Split Columns

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



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Results

New Pivot

✓ 2,168 events (8/26/14 11:00:00.000 PM to 9/2/14 11:30:23.000 PM)

Save As... Clear successful purchase

Filters: Last 7 days, category

Split Columns: product name, Column Values: Count of succe...

The ALL column shows row totals by category

The ALL row shows column totals by product name

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

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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

The screenshot shows two panels of the Splunk 'New Pivot' interface. The left panel displays a table of event counts for categories: ARCADE (120), SHOOTER (0), SIMULATION (0), SPORTS (0), STRATEGY (0), and TEE (0). The right panel shows the configuration of a filter for the 'category' attribute. Step 1 highlights the '+' button to add a new filter. Step 2 highlights the 'category' attribute in the list. Step 3 highlights the 'Match' dropdown set to 'is not'. Step 4 highlights the dropdown menu with 'is not' selected. Step 5 highlights the 'ACCESSORIES' category in the list. Step 6 highlights the 'Add To Table' button at the bottom right.

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

1

2

3

4

5

6

Add To Table

Category	Count
ARCADE	120
SHOOTER	0
SIMULATION	0
SPORTS	0
STRATEGY	0
TEE	0

# Filtered Pivot

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

New Pivot

✓ 1,863 events (8/26/14 11:00:00.000 PM to 9/2/14 11:51:08.000 PM)

Save As... Clear successful purchase

Filters

Last 7 days category is not ...

Split Columns

product name

Documentation

Split Rows

category

Column Values

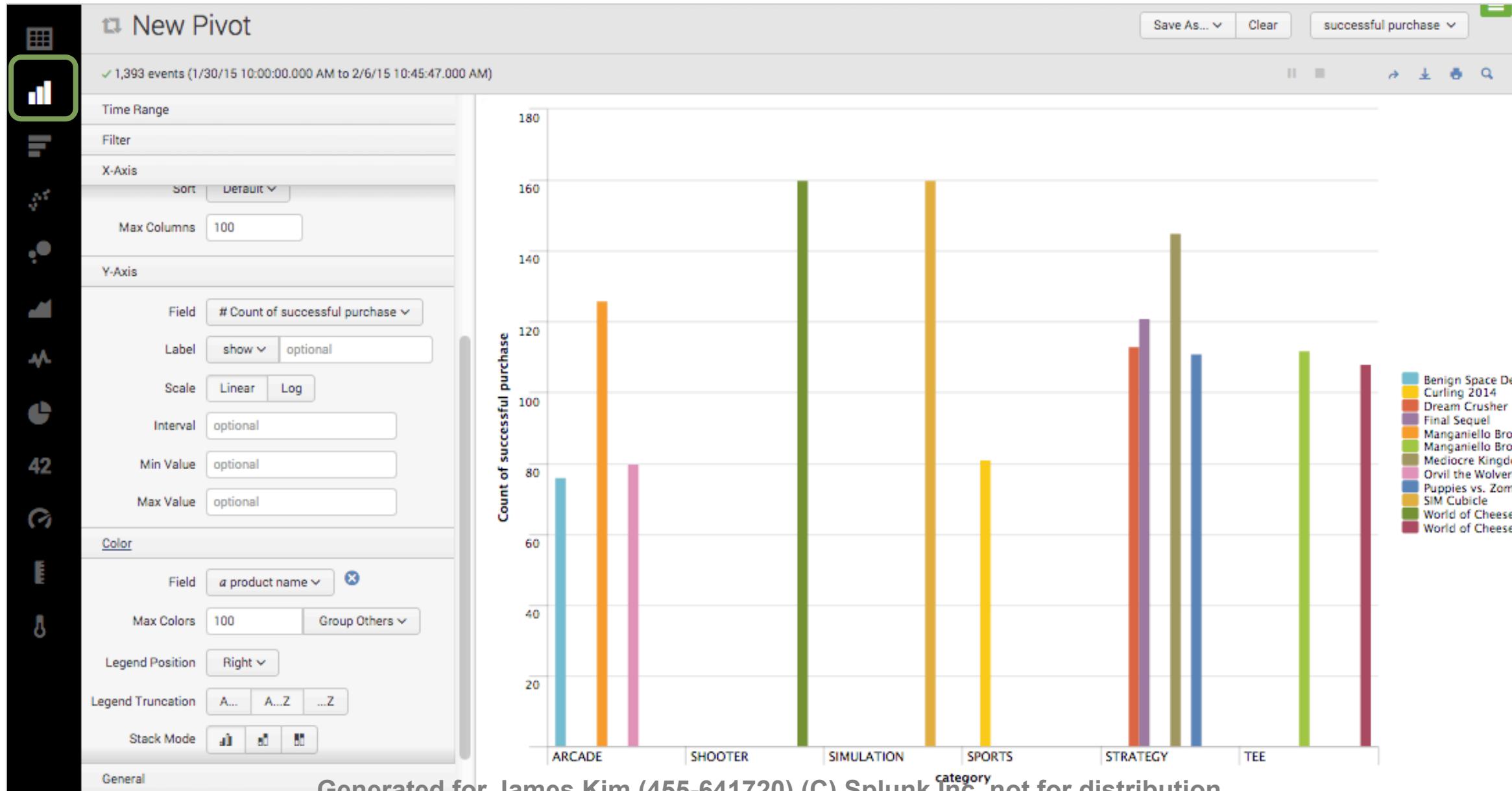
Count of succe...

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

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

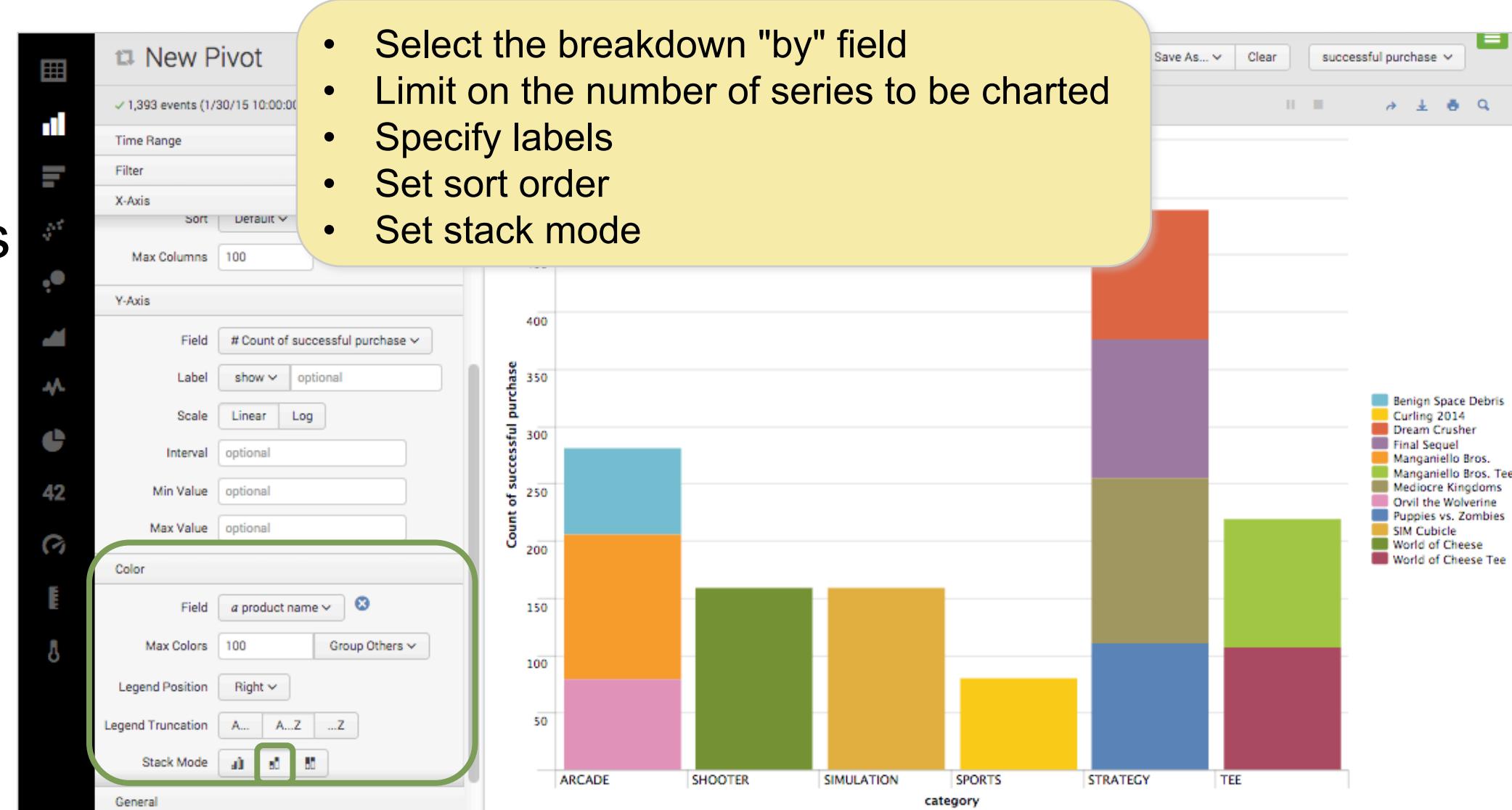
# Select a Visualization Format

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



# Modify Visualization Settings

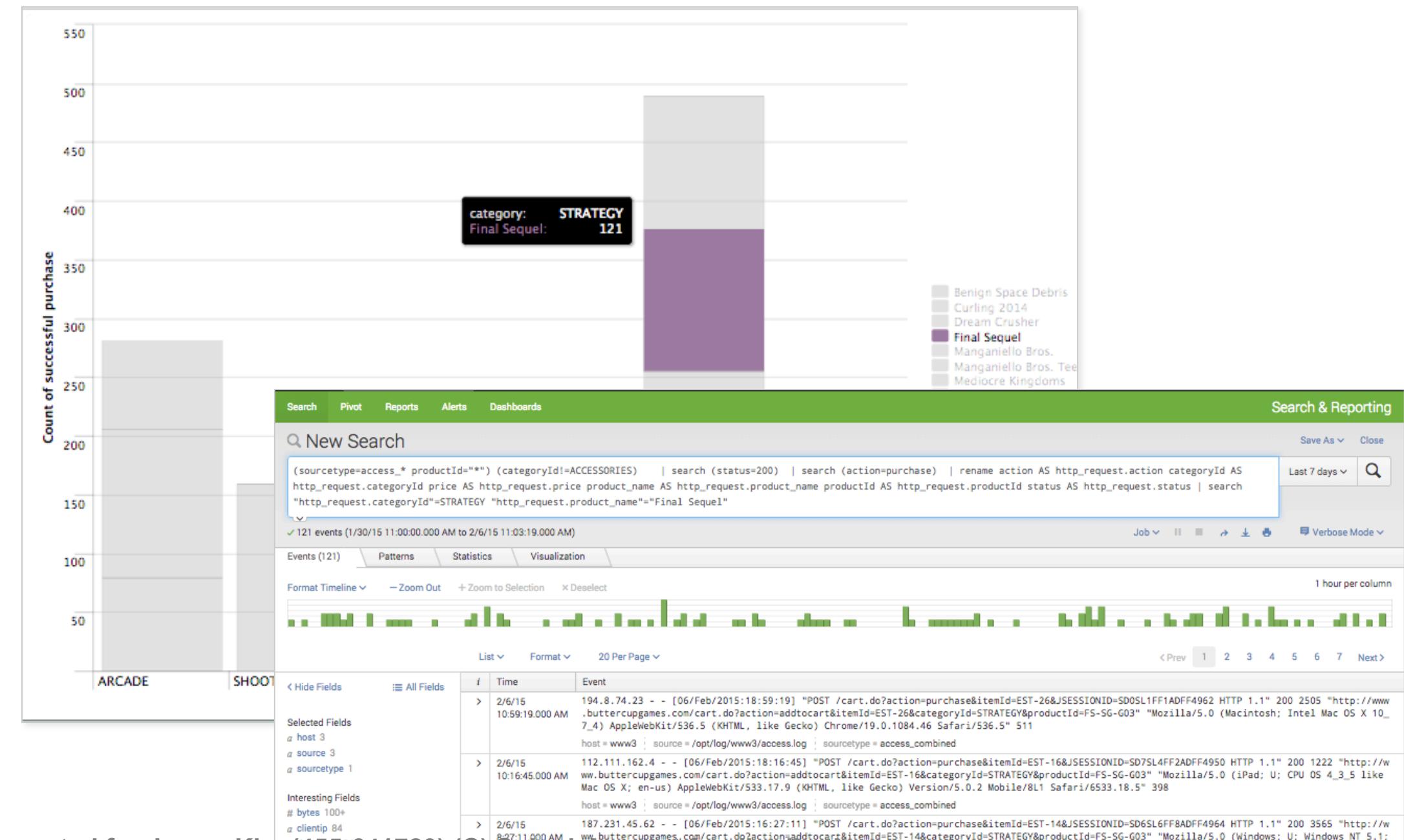
- Notice along the left there are controls that allow you to change visualization settings
- By default, Drilldown is enabled, which means that when an item in the visualization is clicked, its underlying search opens in the Search and Reporting app



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Mouse Actions

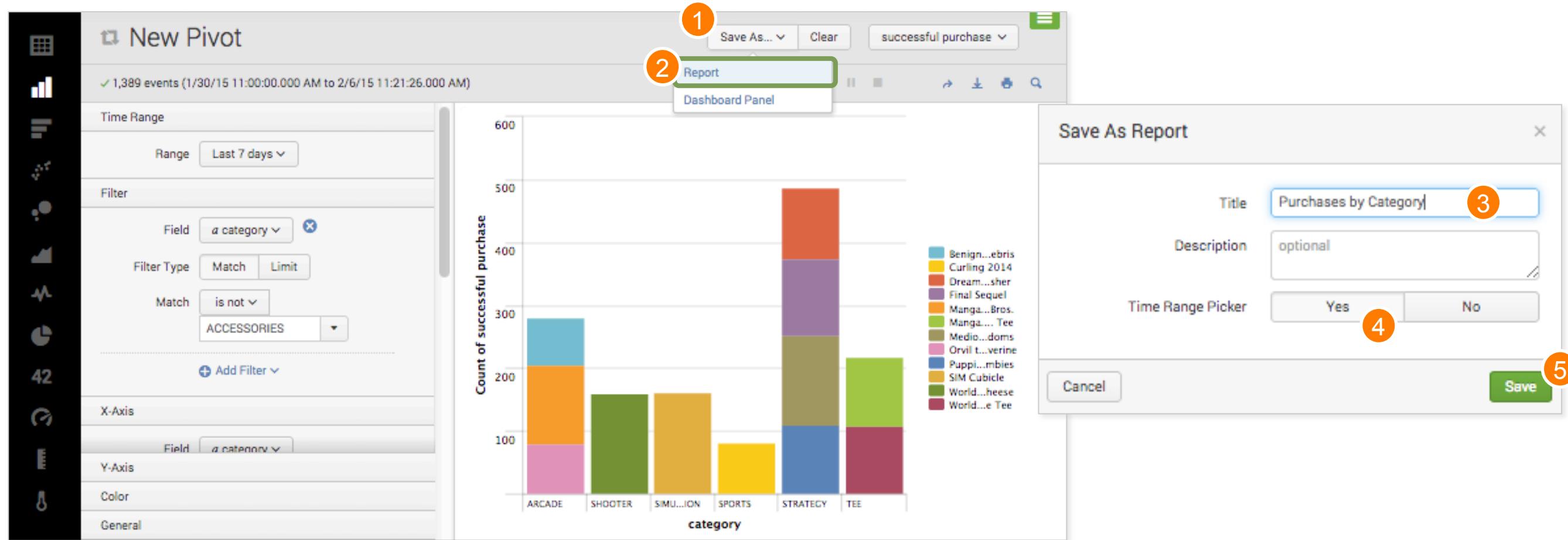
- Mouse over to reveal details
- Click an area to open its underlying search (click is available only if Drilldown remains enabled)



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Save Pivot

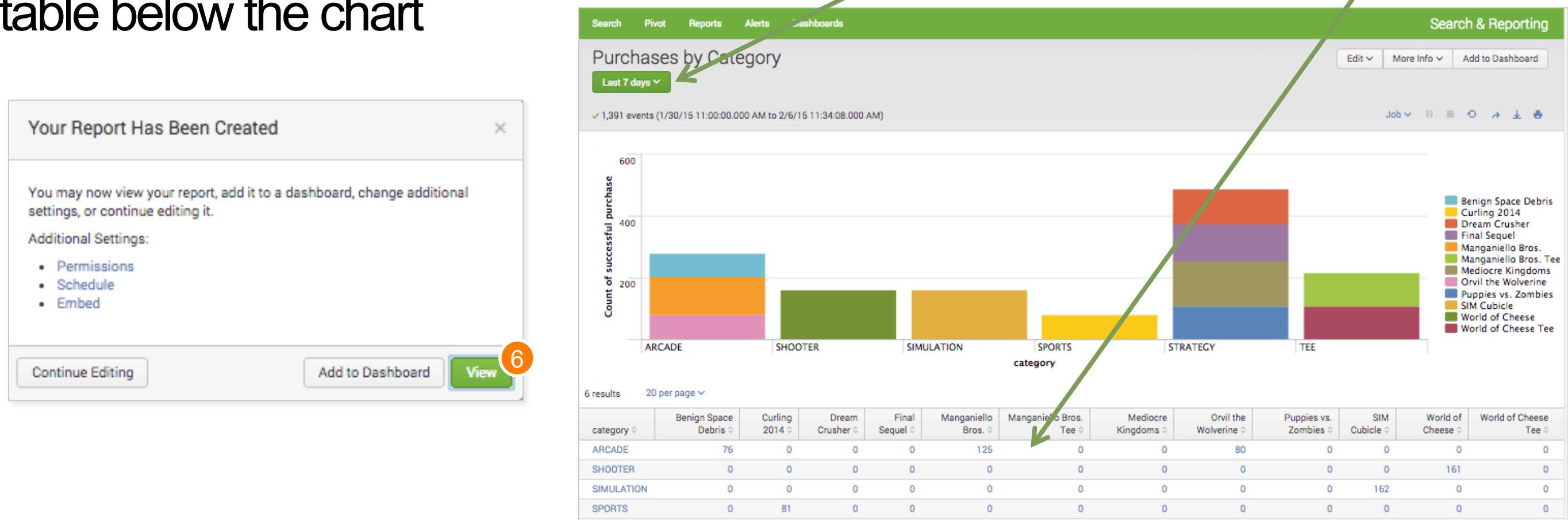
- Pivots are saved as reports or dashboard panels (both taught later in this course)
- You can choose to include a Time Range Picker in the report to allow people who view it to change the time range (default is Yes)



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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



Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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 wish to include in the object
  4. Create a table or visualization in Pivot and save it

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# Open Instant Pivot

The screenshot shows the Splunk Search & Reporting interface. A search bar at the top contains the query `action=purchase`. Below the search bar, the results show 950 events from September 7 to 9, 2014. The 'Events (950)' tab is selected. A green arrow points from the 'Events (950)' tab to a tooltip window. The tooltip has five numbered steps:

1. The search bar containing `action=purchase`.
2. The 'Events (950)' tab.
3. The 'Pivot' icon in the tooltip.
4. The 'All Fields (46)' radio button selected in the 'Fields' dialog.
5. The 'OK' button in the 'Fields' dialog.

The tooltip text reads: "Your search isn't generating any statistic or visualization results. Here are some possible ways to get results." It provides three options: "Pivot" (with a description of building tables and visualizations), "Fields" (with a dialog for selecting fields), and "Search Commands" (with a description of using transforming search commands like timechart or stats).

Generated for James Kim (455-641720) (C) Splunk Inc, not for distribution

# 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](http://answers.splunk.com)  
Post specific questions and get them answered by Splunk community experts.
- **Splunk Docs:** [docs.splunk.com](http://docs.splunk.com)  
These are constantly updated. Be sure to select the version of Splunk you are using.
- **Wiki:** [wiki.splunk.com](http://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.