
KOENIG
step forward


splunk>
TM

KOENIG
step forward

Course-Ware

-> Introduction
-> Splunk Inc
-> Licensing
-> Installation
-> Login
-> Splunk Home
-> Getting Data
-> Search Dashboard
-> Data Summary
-> Search Actions and Modes
-> Search Language
-> Using Sub search
-> Field Lookups
-> Saving and Sharing Reports
-> More Searches and Reports
-> Creating Dashboards

KOENIG
step forward

INTRODUCTION

- Splunk Enterprise is the leading platform for real-time operational intelligence. It's the easy, fast and secure way to search, analyze and visualize the massive streams of machine data generated by your IT systems and technology infrastructure—physical, virtual and in the cloud.

- Troubleshoot application problems and investigate security incidents in minutes instead of hours or days, avoid service degradation or outages, deliver compliance at lower cost and gain new business insights

KOENIG
step forward

INTRODUCTION

Feature	Description
Indexing	Splunk indexes machine data. This includes data streaming from packaged and custom applications, application servers, web servers, databases, networks, virtual machines, telecoms equipment, operating systems, sensors, and so on, that make up your IT infrastructure. The maximum indexing volume depends on the Splunk Enterprise license.
Data model	A data model is a hierarchically-structured search-time mapping of semantic knowledge about one or more datasets. It encodes the domain knowledge necessary to build a variety of specialized searches of those datasets. These specialized searches are used by Splunk Enterprise to generate reports for Pivot users. Data model objects represent different datasets within the larger set of data indexed by Splunk Enterprise.
Pivot	Pivot refers to the table, chart, or data visualization you create using the Pivot Editor. The Pivot Editor lets users map attributes defined by data model objects to a table or chart data visualization without having to write the searches to generate them. Pivots can be saved as reports and added to dashboards.

KOENIG
step forward

INTRODUCTION

Search	an Index, use statistical commands to calculate metrics and generate reports, search for specific conditions within a rolling time window, identify patterns in your data, predict future trends, and so on. Searches can be saved as reports and used to power dashboard panels.
Alerts	Alerts are triggered when conditions are met by search results for both historical and real-time searches. Alerts can be configured to trigger actions such as sending alert information to designated email addresses, post alert information to an RSS feed, and run a custom script, such as one that posts an alert event to syslog.
Reports	Reports are saved searches and pivots. You can run reports on an ad hoc basis, schedule them to run on a regular interval, set a scheduled report to generate alerts when the results of their runs meet particular conditions. Reports can be added to dashboards as dashboard panels.
Dashboards	Dashboards are made up of panels that contain modules such as search boxes, fields, charts, tables, forms, and so on. Dashboard panels are usually hooked up to saved searches or pivots. They can display the results of completed searches as well as data from backgrounded real-time searches.

KOENIG
step forward

SPLUNK INC.

- Founded in 2003 and headquartered in San Francisco, California
- **Specialties –** "Machine Data To Operational Intelligence" –
  The machine data that facilitates operational intelligence comes in many different from many different sources. Splunk is able to collect and index data from many different sources, including logfiles written by web servers or business applications, syslog data streaming in from network devices, or the output of custom developed scripts.
- Searching, monitoring, and analyzing machine-generated big data, via a web-style interface
- According to tech target, Splunk is designated as the SIEM of the year.
- The name "Splunk" is a reference to exploring caves, as in spelunking.

KOENIG
step forward

SPLUNK – LICENSING

- You'll get a Splunk Enterprise **FREE** license for 60 days and you can index up to 500 megabytes of data per day.

- **Perpetual and Term Licensing**

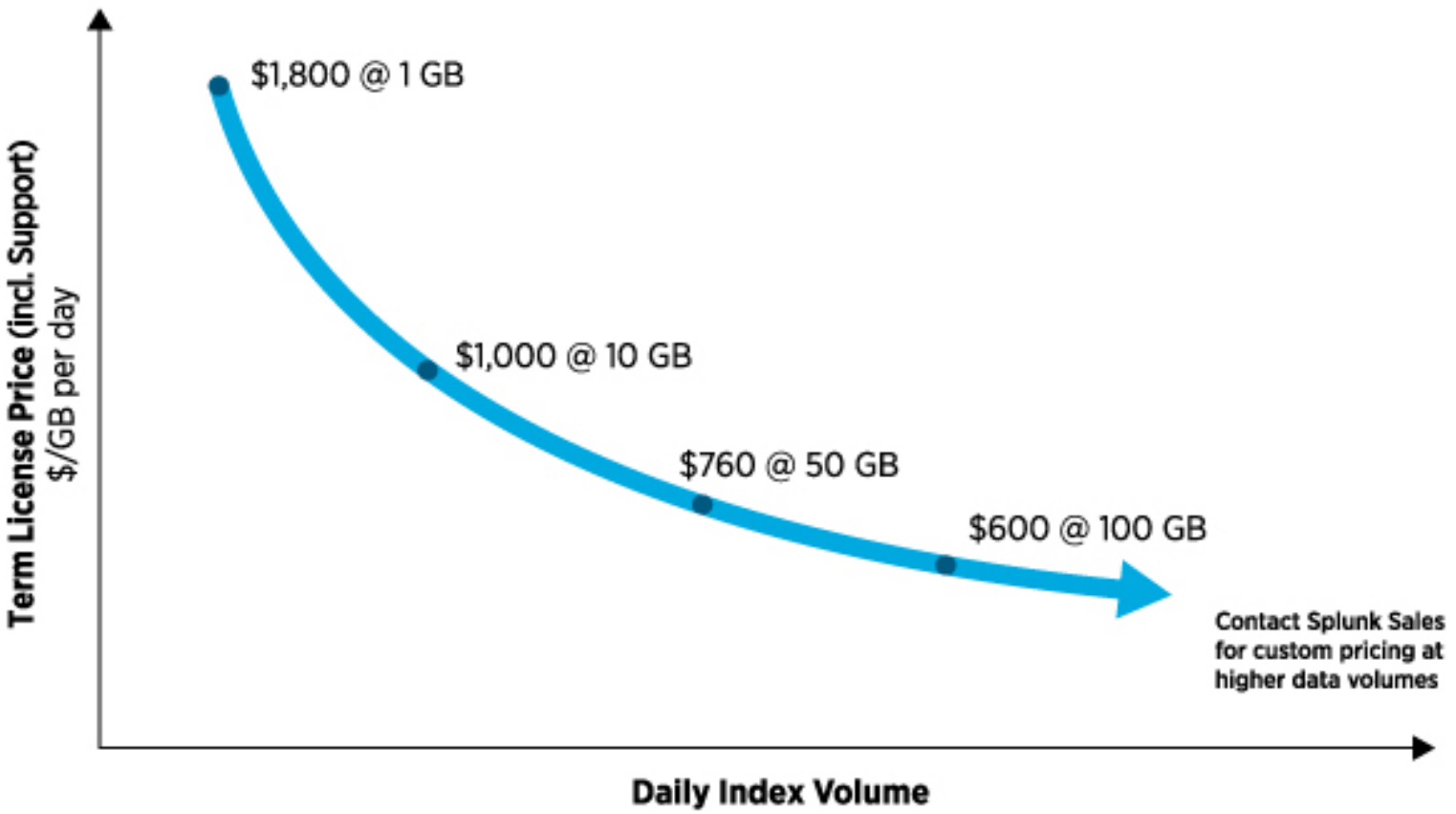
  There are two options for licensing Splunk Enterprise:

  Perpetual license: this includes the full functionality of Splunk Enterprise and starts as low as $4,500 for 1 GB/day*, plus annual support fees.

  Term license: this provides the option of paying a yearly fee instead of the one-time perpetual license fee. Term licenses start at $1,800 per year*, which includes annual support fees.

KOENIG
step forward

SPLUNK – LICENSING



KOENIG
step forward

INSTALLATION

- **Linux** installation instructions

  tar xvzf splunk_package_name.tgz -C /opt

- **Windows** installation instructions

1. To start the installer, double-click the splunk.msi file.
2. In the Welcome panel, click Next.
3. In Customer Information, enter the requested details and click Next.
4. Splunk Enterprise is installed by default into the \Program Files\Splunk directory.

KOENIG
step forward

INSTALLATION

- **Mac OS X installation instructions**

1. Navigate to the folder or directory where the installer is located.

2. Double-click on the DMG file.

3. Double-click on splunk.pkg.

4. Choose a location to install Splunk.

5. Click Install.

The installer places a shortcut on the Desktop.

KOENIG
step forward

Users

- About Splunk Enterprise users

Persona	Industry Role	Activities
Administrator	network engineer, system administrator	• Configures, administers, optimizes, and secures the Splunk Enterprise deployment. • Sets up user accounts and permissions. • Gets data into Splunk Enterprise.
Knowledge Manager	data analyst, system administrator	• Oversees knowledge object creation, normalization, and usage across teams, departments, and deployments. • Gets the data into Splunk, or works with the administrator to do so. • Creates and shares data models.
Search User	data analyst, IT professional, network engineer, security analyst, system administrator	• Uses Search to investigate server problems, understand configurations, monitor user activities, and troubleshoot escalated problems. • Builds reports and dashboards to monitor the health, performance, activity, and capacity of their IT infrastructure. • Identifies patterns and trends that are indicators of routine problems.

KOENIG
step forward

Users

- About Splunk Enterprise users

Pivot User	business professional, data analyst, executive, IT professional, manager, system administrator	• Uses Pivot to build reports based on data models created by the Knowledge Manager. • Creates reports and dashboards to monitor their businesses. • Identifies trends in the health and performance of their businesses.
Developer	system integrator, professional developer	• Integrates data and functionality of applications with Splunk Enterprise. • Builds Splunk Apps and add-ons with custom dashboards and data visualizations.

KOENIG
step forward

First time Login

- The Splunk interface is web-based, which means that no client needs to be installed.

  http://localhost:8000

- First time signing credentials

  Username – admin

  Password - changeme

  It is a good idea to change this password to prevent unwanted changes to your deployment.

KOENIG
step forward

Splunk Home

- **Apps**

  The Apps panel lists the apps that are installed on your Splunk instance that you have permission to view. Select the app from the list to open it.

  For an out-of-the-box Splunk Enterprise installation, you see one App in the workspace: Search & Reporting. When you have more than one app, you can drag and drop the apps within the workspace to rearrange them.

- You can do two actions on this panel:

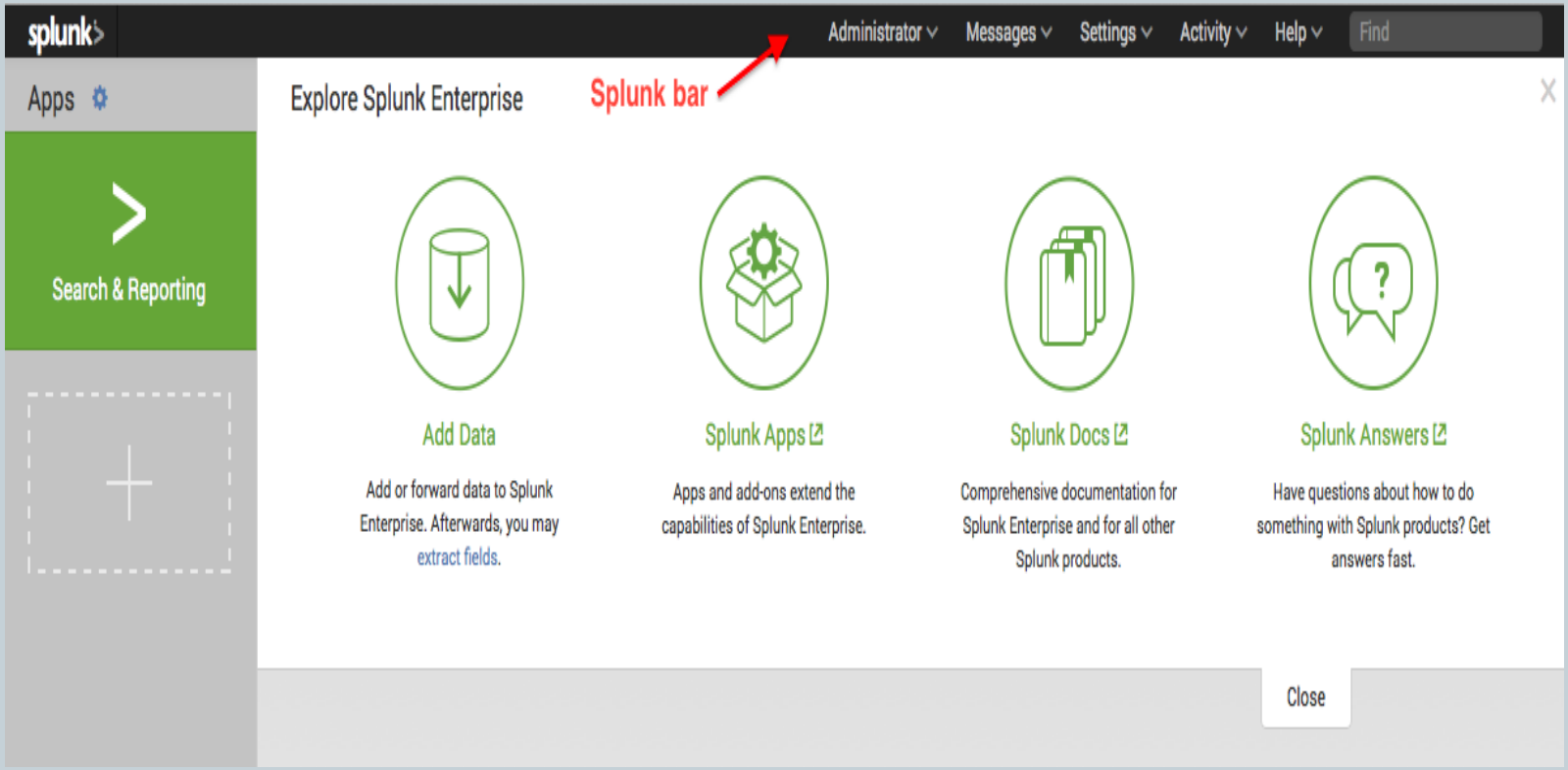
  - Click the gear icon to view and manage the apps that are installed in your Splunk instance.

  - Click the plus icon to browse for more apps to install.

KOENIG
step forward

Splunk Home

- Splunk Bar



KOENIG
step forward

Splunk Home

- **Settings menu**

  The Settings menu lists the configuration pages for Knowledge objects, Distributed environment settings, System and licensing, Data, and Authentication settings. If you do not see some of these options, you do not have the permissions to view or edit them.

- **User menu**

  The User menu here is called "Administrator" because that is the default user name for a new installation. You can change this display name by selecting Edit account and changing the Full name. You can also edit the time zone settings, select a default app for this account, and change the account's password. The User menu is also where you Logout of this Splunk installation.

KOENIG
step forward

Splunk Home

- **Messages menu**

  All system-level error messages are listed here. When there is a new message to review, a notification displays as a count next to the Messages menu.

- **Activity menu**

  -Click Jobs to open the search jobs manager window, where you can view and manage currently running searches.

  -Click Triggered Alerts to view scheduled alerts that are triggered. This tutorial does not discuss saving and scheduling alerts.

  -Click System Activity to see Dashboards about user activity and status of the system.

KOENIG
step forward

GETTING DATA

- A Splunk data repository is called an index. During indexing (or event processing), Splunk processes the incoming data stream to enable fast search and analysis, storing the results in the index as events.

- Events are stored in the index as a group of files that fall into two categories:

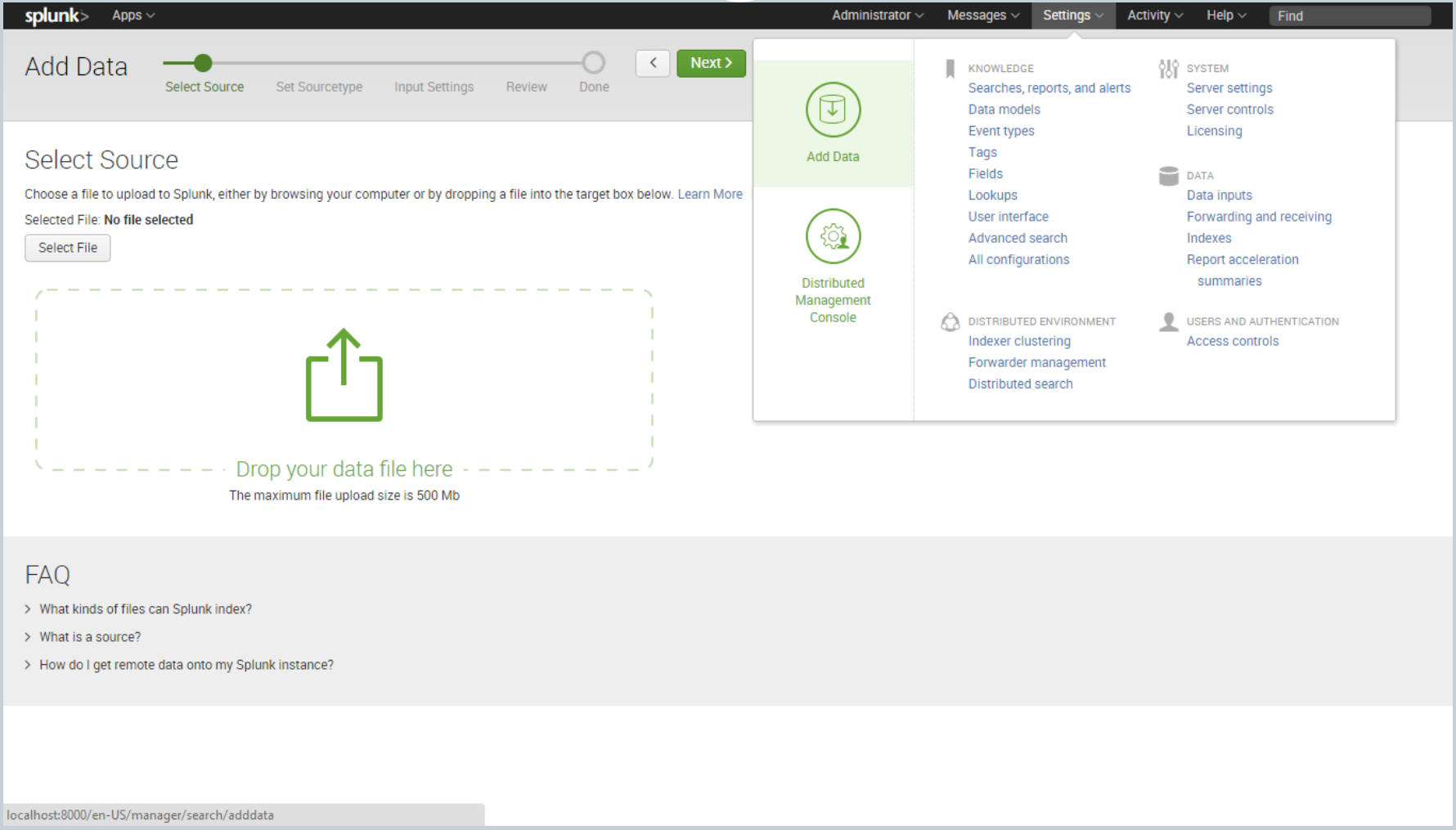
  - Rawdata, which is the raw data in a compressed form.

  - Index files and some metadata files that point to the raw data.

- These files reside in sets of directories, called buckets, organized by age.

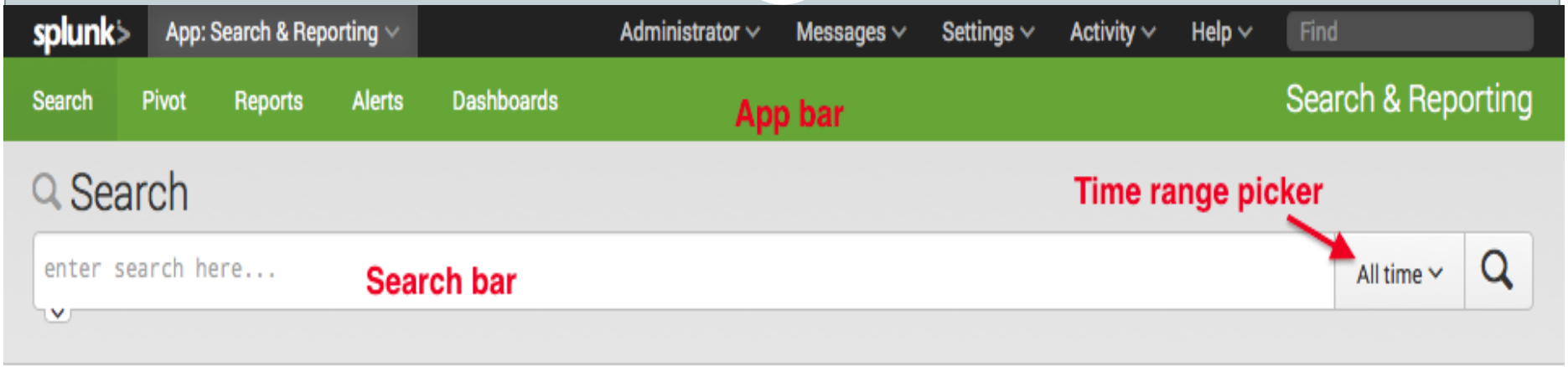
KOENIG
step forward

GETTING DATA



KOENIG
step forward

SEARCH DASHBOARD



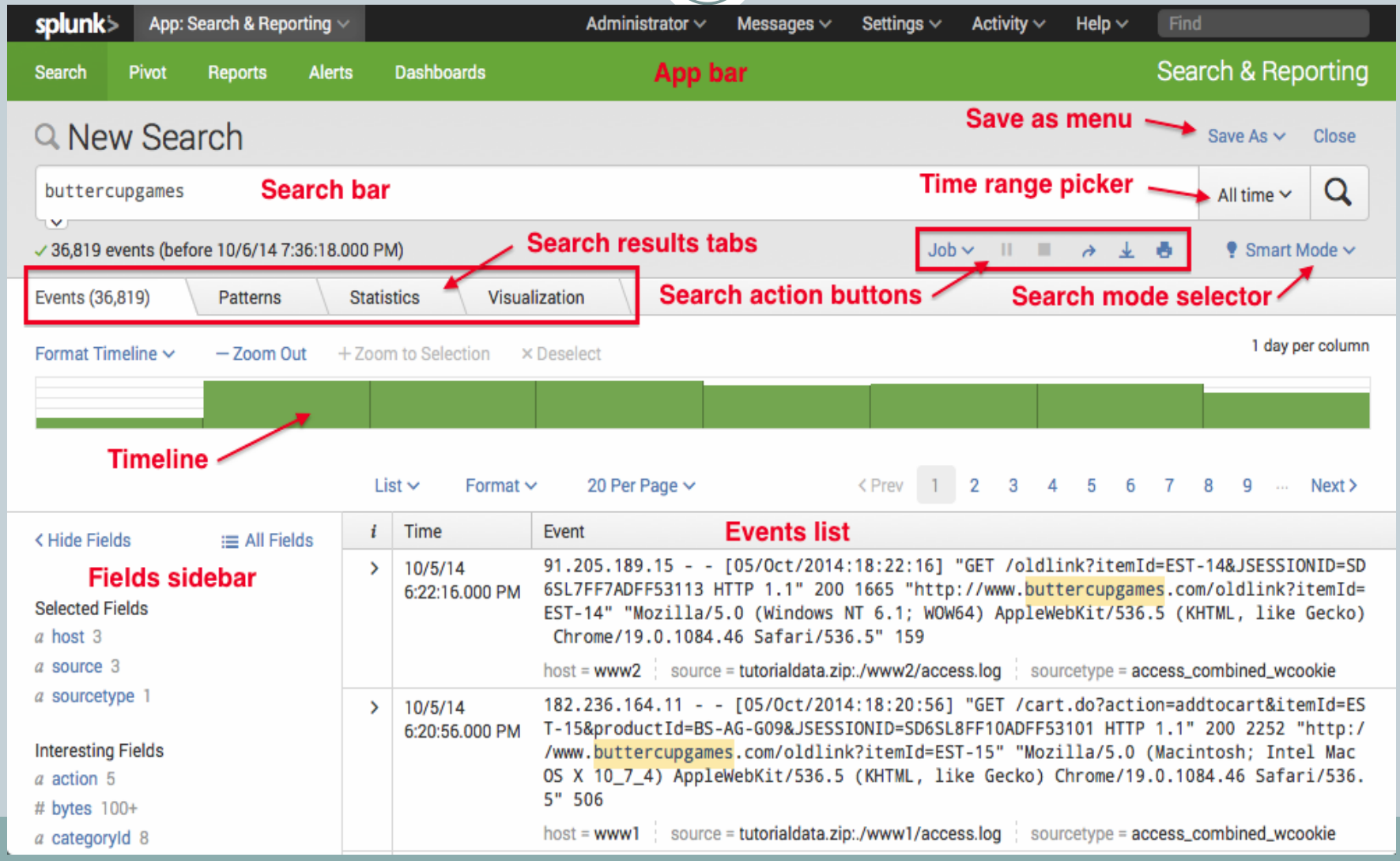
KOENIG
step forward

DATA SUMMARY

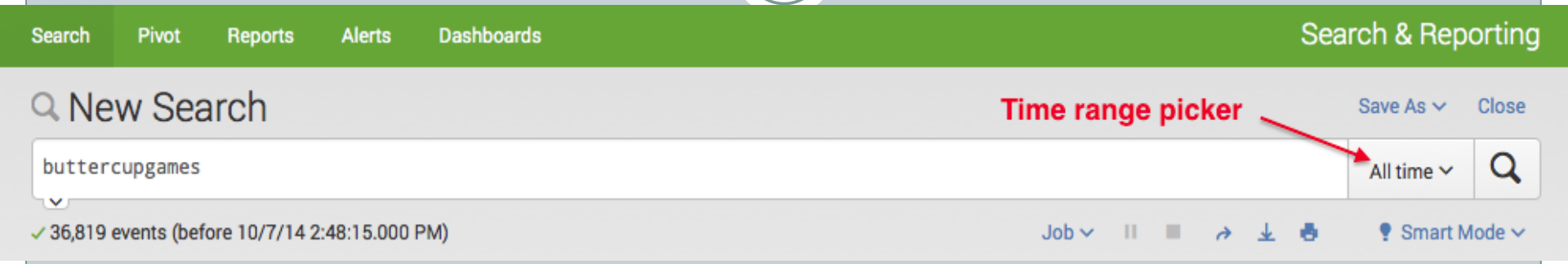
- The Data Summary dialogue displays three tabs: Hosts, Sources, Sourcetypes.
- The host of an event is the host name, IP address, or fully qualified domain name of the network machine from which the event originated.
- The source of an event is the file or directory path, network port, or script from which the event originated.
- The source type of an event tells you what kind of data it is, usually based on how it is formatted. This classification lets you search for the same type of data across multiple sources and hosts.

KOENIG
step forward

DATA SUMMARY



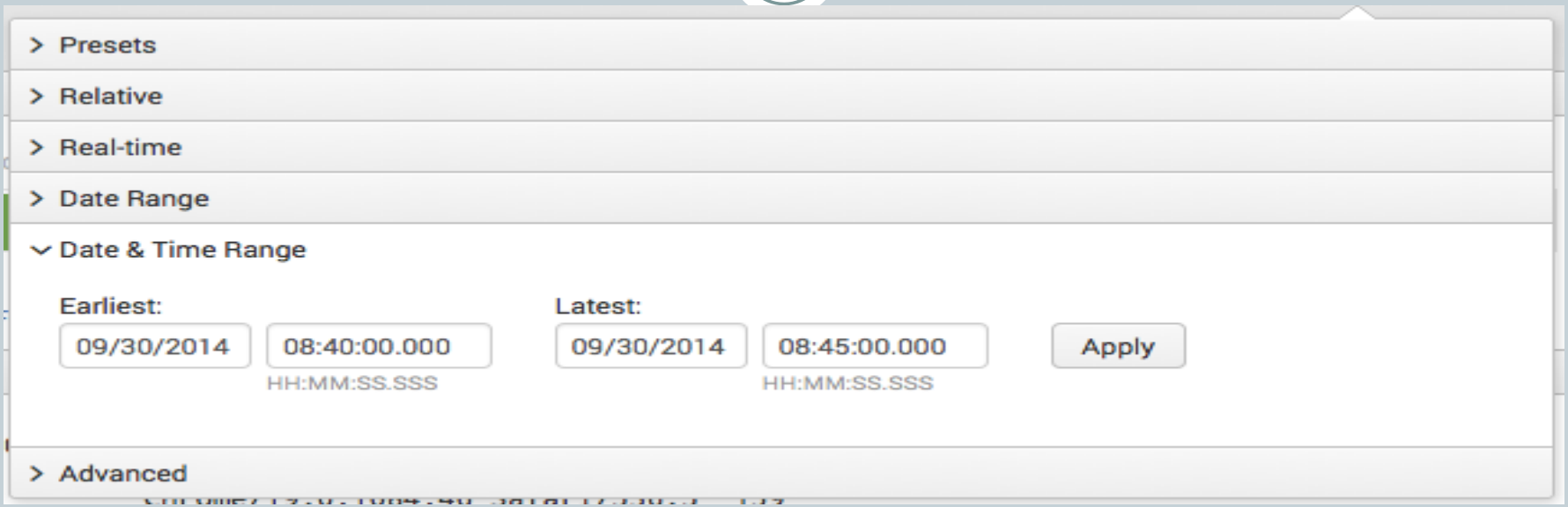
Time Range Picker



- By default, the time range for a search is set to All time. When you search large volumes of data, results return faster when you run the search over a smaller time period.
- If one of the Presets is not what you want, you can define a custom time range, such as a Relative time range or a Date & Time Range.

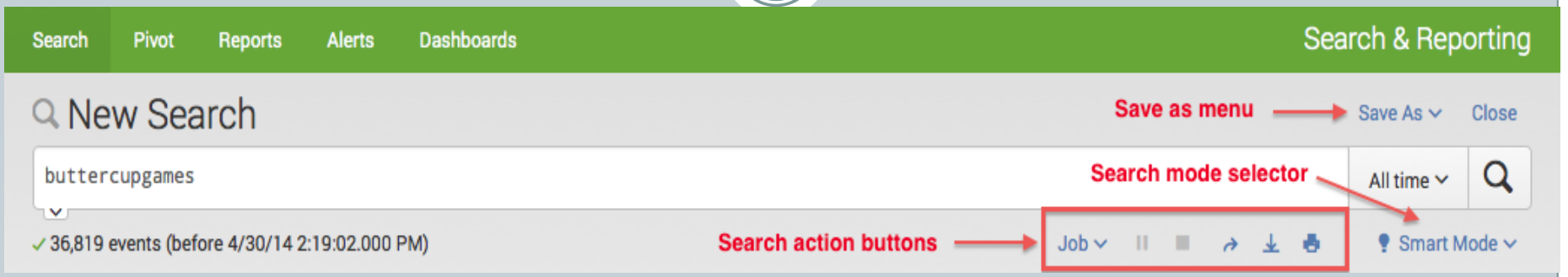
  To run a search over the last two hours, use the Relative time range option.

Time Range Picker



- For example, to troubleshoot an issue that took place September 30th at 8:42 PM, you can specify the earliest time to be 09/30/2014 08:40:00.000 and the latest time to be 09/30/2014 08:45:00.000.

Search Actions and Modes



- Control search job progress

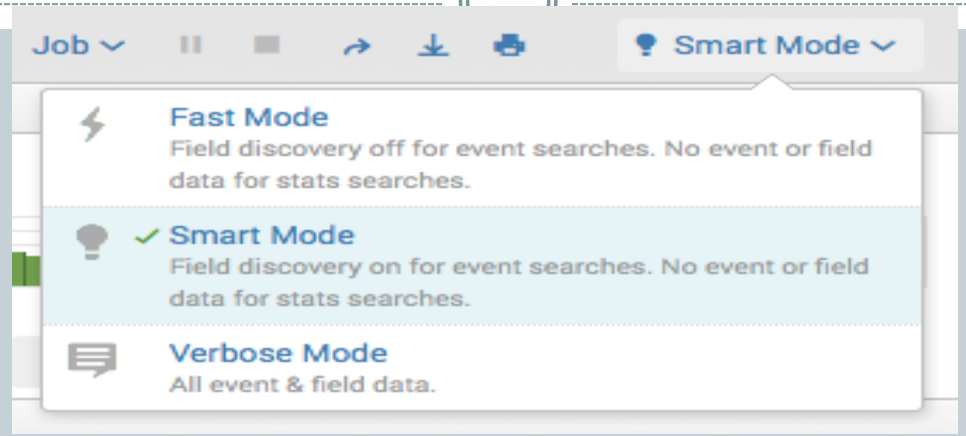
  After you launch a search, you can pause it and stop it using the buttons under the search bar. Also, you can access and manage information about the search's job without leaving the Search page.

Search Actions and Modes

- Click Job and choose from the available options there.

- **Edit job settings.** Select this option to open the Job Settings dialog box, where you can change the job's read permissions, extend the job's lifespan, and get a URL for the job that you can use to share the job with others or put a link to the job in your browser's bookmark bar.
- **Send job to the background.** Select this option if the search job is slow and you want to run the job in the background while you work on other Splunk Enterprise activities (including running a new search job).
- **Inspect job.** Opens a separate window and displays information and metrics for the search job using the Search Job Inspector.
- **Delete job.** Use this option to delete a job that is running, is paused, or which has finalized. After you delete the job, you can save the search as a report.

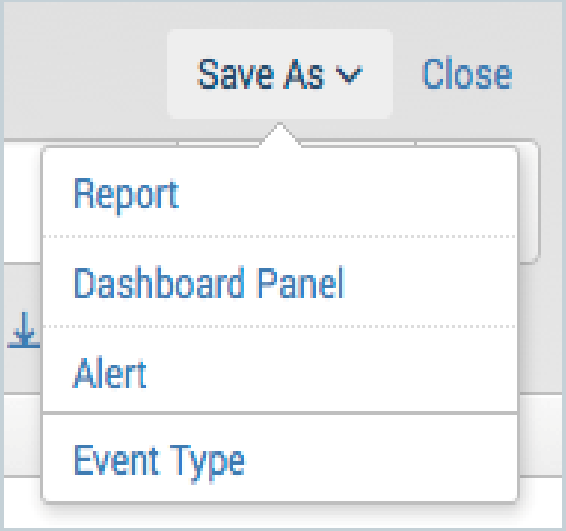
Search Actions and Modes



- The Search mode controls the search experience. You can set it to speed up searches by cutting down on the event data it returns (Fast mode), or you can set it to return as much event information as possible (Verbose mode). In Smart mode (the default setting) it toggles search behavior based on the type of search you're running.

Search Actions and Modes

- Save the results
- The Save as menu lists options for saving the results of a search as a Report, Dashboard Panel, Alert, and Event type.



KOENIG
step forward

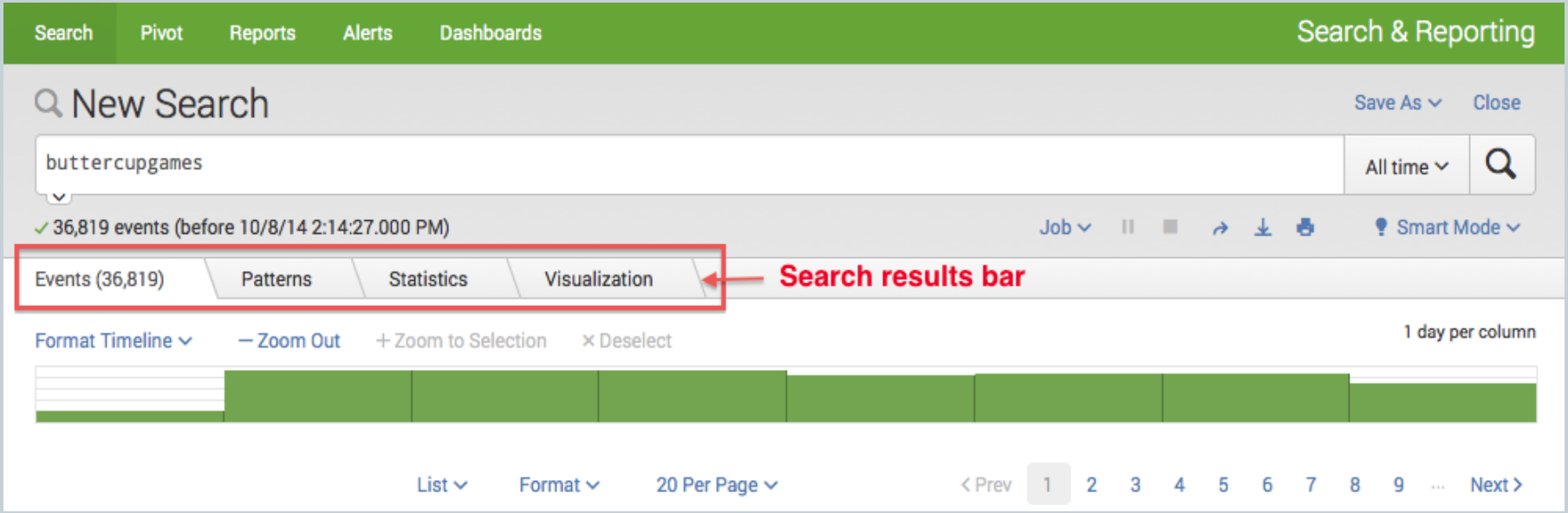
Search Actions and Modes

- Other search actions

- The **Share** options shares the search job. This option extends the job's lifetime to seven days and set the read permissions to Everyone.
- The **Export** option exports the results. Select this option to output to CSV, raw events, XML, or JSON and specify the number of results to export.
- The **Print** option sends the results to a printer that has been configured.

Search Actions and Modes

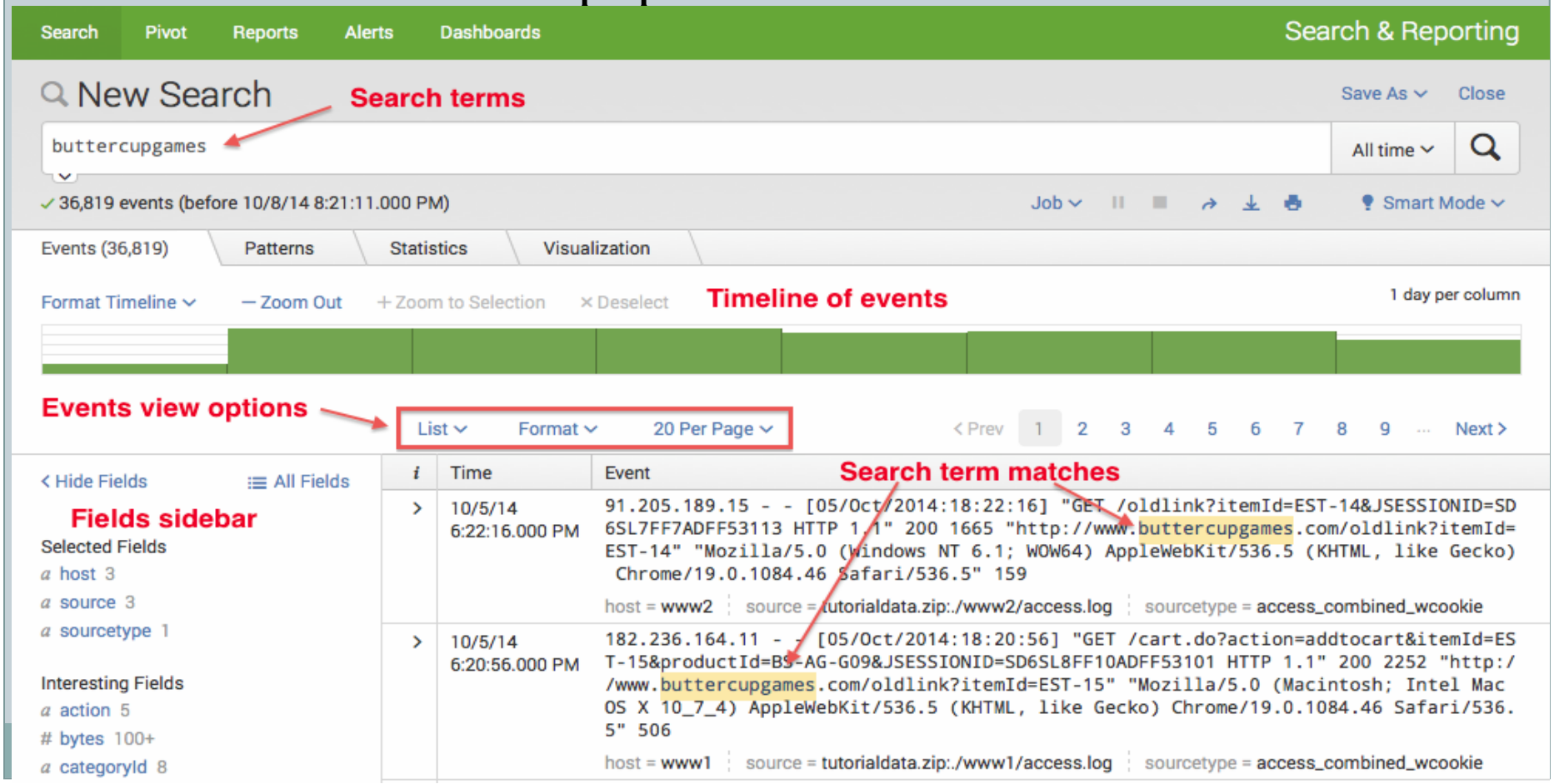
- Search Results Tabs



- If your search retrieves events, you can view the results in the Events tab and the Patterns tab, but not in the other tabs. If your search includes transforming commands, you can view the results in the Statistics and Visualization tabs.

Search Actions and Modes

- Events - The keyword search used in this screenshot retrieves events and populates the Events results tab.



KOENIG
step forward

Search Actions and Modes

- The Events tab displays the timeline of events, the fields sidebar, and the events viewer. To change the event view, use the List and Format options. By default, the events appear as a list that is ordered starting with the most recent event. In each event, the matching search terms are highlighted.

KOENIG
step forward

Search Actions and Modes

- **Timeline of events:** A visual representation of the number of events that occur at each point in time. As the timeline updates with your search results, you might notice clusters or patterns of bars. The height of each bar indicates the count of events. Peaks or valleys in the timeline can indicate spikes in activity or server downtime. Thus, the timeline highlights patterns of events or investigates peaks and lows in event activity. The timeline options are located above the timeline. You can zoom in, zoom out, and change the scale of the chart.

KOENIG
step forward

Search Actions and Modes

- **Timeline of events:** A visual representation of the number of events that occur at each point in time. As the timeline updates with your search results, you might notice clusters or patterns of bars. The height of each bar indicates the count of events. Peaks or valleys in the timeline can indicate spikes in activity or server downtime. Thus, the timeline highlights patterns of events or investigates peaks and lows in event activity. The timeline options are located above the timeline. You can zoom in, zoom out, and change the scale of the chart.

KOENIG
step forward

Search Actions and Modes

- **Fields sidebar**: When you index data, Splunk by default extracts information from your data that is formatted as name and value pairs, which we call fields. When you run a search, Splunk lists all of the fields it discovers in the fields sidebar next to your search results. You can select other fields to show in your events. Also, you can hide this sidebar and maximize the results area.

- Selected fields are set to be visible in your search results. By default, host, source, and sourcetype appear.
- Interesting fields are other fields that Splunk has extracted from your search results.

KOENIG
step forward

Search Actions and Modes

- **Patterns**

  The Patterns tab simplifies event pattern detection. It displays a list of the most common patterns among the set of events returned by your search. Each of these patterns represents a number of events that all share a similar structure.
- **You can click on a pattern to:**
- View the approximate number of events in your results that fit the pattern.
- See the search that returns events with this pattern.
- Save the pattern search as an event type, if it qualifies.
- Create an alert based on the pattern.

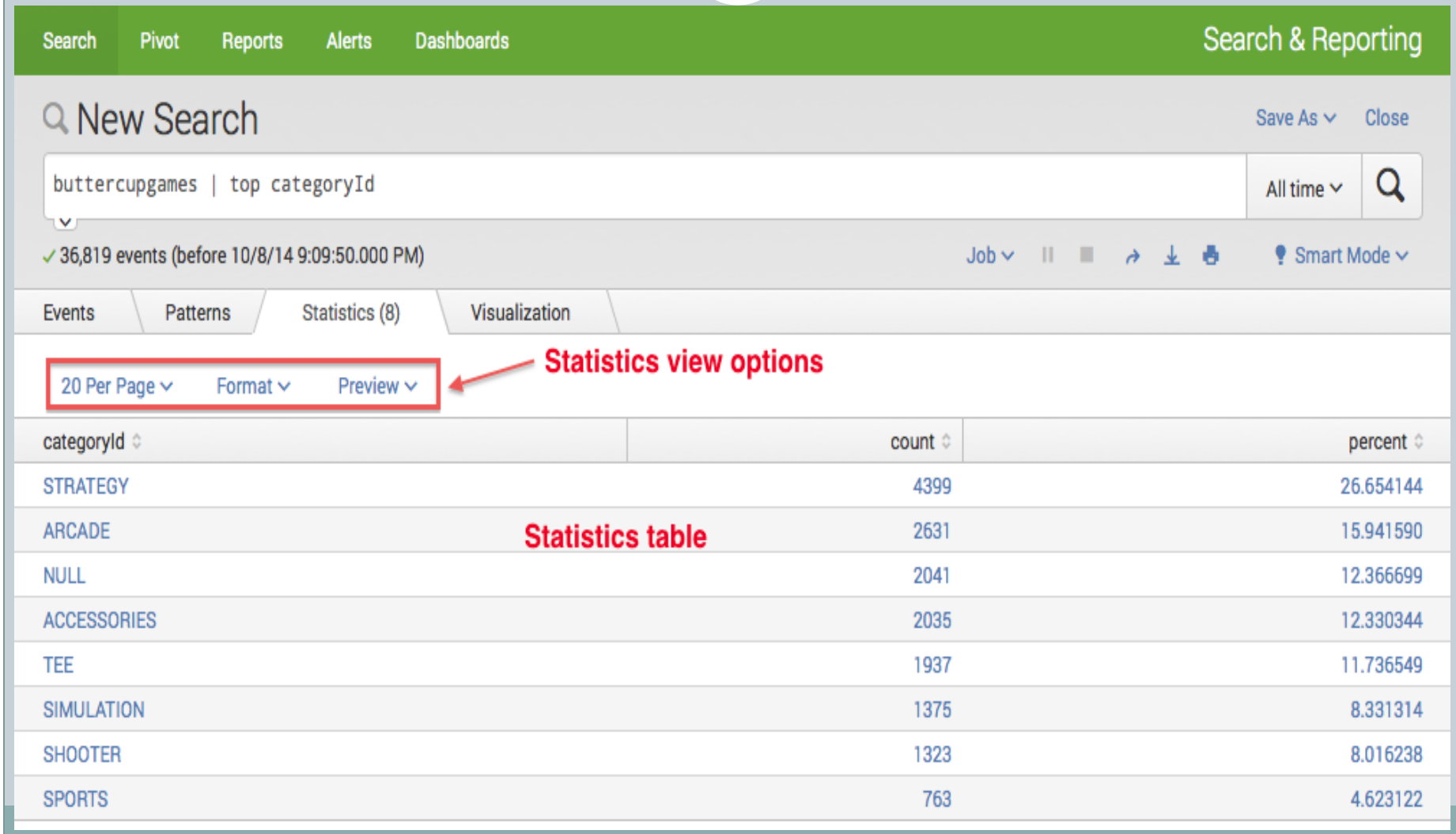
KOENIG
step forward

Search Actions and Modes

- **Statistics**
- The Statistics tab populates when you run a search with transforming commands such as stats, top, chart, and so on. The previous keyword search for "buttercupgames" does not display any results in this tab because it does not have any transforming commands.
- With a transforming search, such as one to find the popular categories of items sold on the Buttercup Games online store, the Statistics tab displays a table of results.

KOENIG
step forward

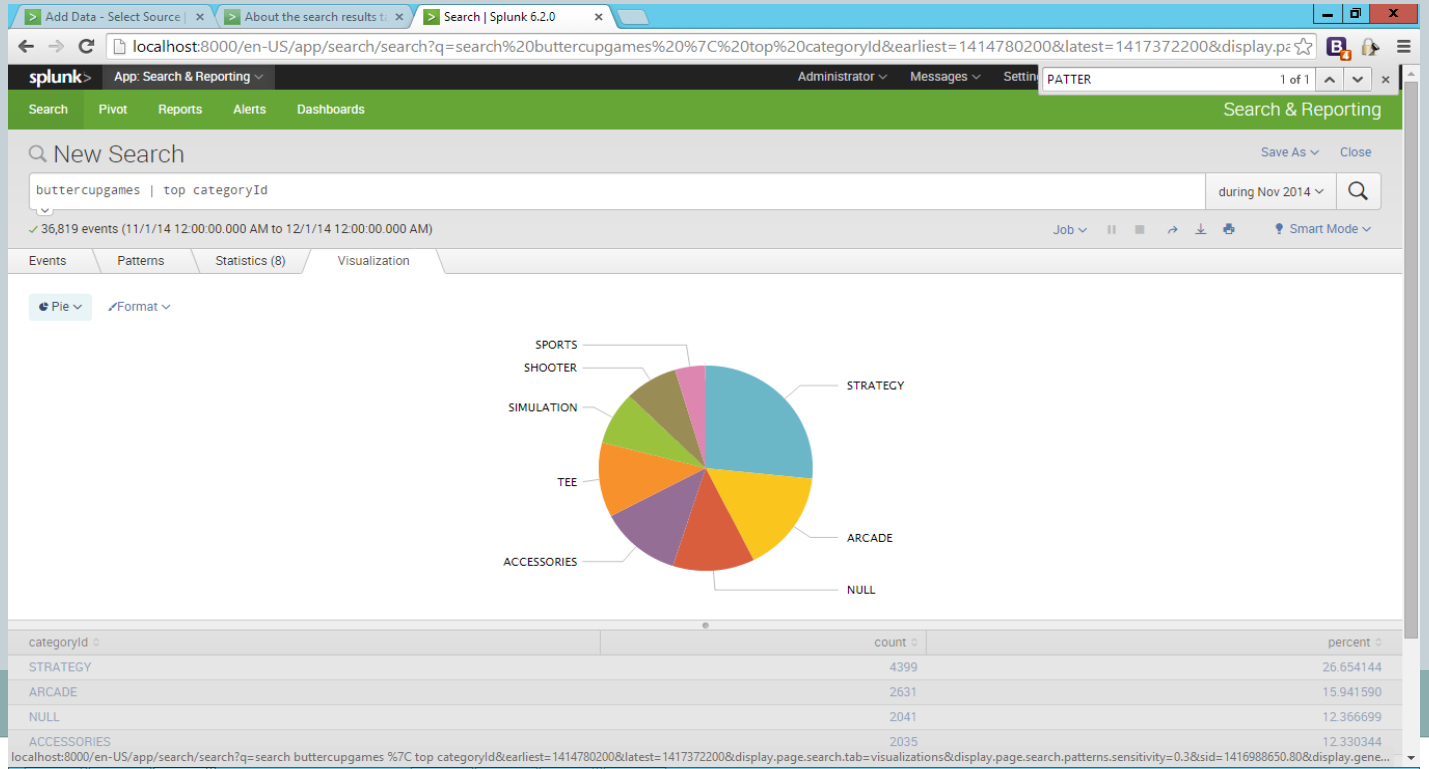
Search Actions and Modes



Search Actions and Modes

- **Visualizations**

  Transforming searches also populate the Visualization tab. The results area of the Visualizations tab includes a chart and the statistics table used to generated the chart. By default, the visualization type is the Columnchart.



KOENIG
step forward

Start Searching

- **Retrieve events from the index**
- 1. Type in keywords to find errors or failures and use Boolean operators: AND, OR, NOT.
- EXAMPLE: buttercupgames (error OR fail* OR severe)
- Boolean operators need to be capitalized. The AND directive is implied between terms, so you do not need to write it. You can use parentheses to group terms. When evaluating boolean expressions, precedence is given to terms inside parentheses. AND or NOT clauses are evaluated before OR clauses. The asterisk wildcard is used to match terms that start with "fail". These terms can include: failure, failed, and so on.

KOENIG
step forward

Start Searching

- **Use fields to search**

- Fields exist in machine data in many forms. Often, a field is a value (with a fixed, delimited position on the line) or a name and value pair, where there is a single value to each field name. A field can be multivalued, that is, it can appear more than once in an event and has a different value for each appearance.
- Some examples of fields are clientip for IP addresses accessing your Web server, _time for the timestamp of an event, and host for domain name of a server. One of the more common examples of multivalue fields is email address fields. While the From field will contain only a single email address, the To and Cc fields have one or more email addresses associated with them.
- In Splunk Enterprise, fields are searchable name and value pairings that distinguish one event from another because not all events will have the same fields and field values. Fields let you write more tailored searches to retrieve the specific events that you want.

KOENIG
step forward

Start Searching

- **Find and select fields**
- SEARCH BAR: sourcetype="access_*“

  Search for fields use the syntax: fieldname="fieldvalue" . Field names are case sensitive, but field values are not. You can use wildcards in field values. Quotes are required when the field values include spaces.

  This search indicates that you want to retrieve only events from your web access logs and nothing else.

  This search uses the wildcard access_* to match any Apache web access sourcetype, which can be access_common, access_combined, or access_combined_wcookie.
- **In the Events tab, scroll through the list of events.**

- If you are familiar with the access_combined format of Apache logs, you recognize some of the information in each event, such as:
- IP addresses for the users accessing the website.
- URIs and URLs for the pages requested and referring pages.
- HTTP status codes for each page request.
- GET or POST page request methods.

KOENIG
step forward

Start Searching

List ▾ Format ▾ 20 Per Page ▾ ‹ Prev 1 2 3 4 5 6 7 8 9 … Next ›

‹ Hide Fields ☰ All Fields

Selected Fields
a host 3
a source 3
a sourcetype 1

Interesting Fields
a action 5
bytes 100+
a categoryId 8
a clientip 100+
date_hour 24
date_mday 8
date_minute 60
a date_month 1
date_second 60
a date_wday 7
date_year 1
a date_zone 1

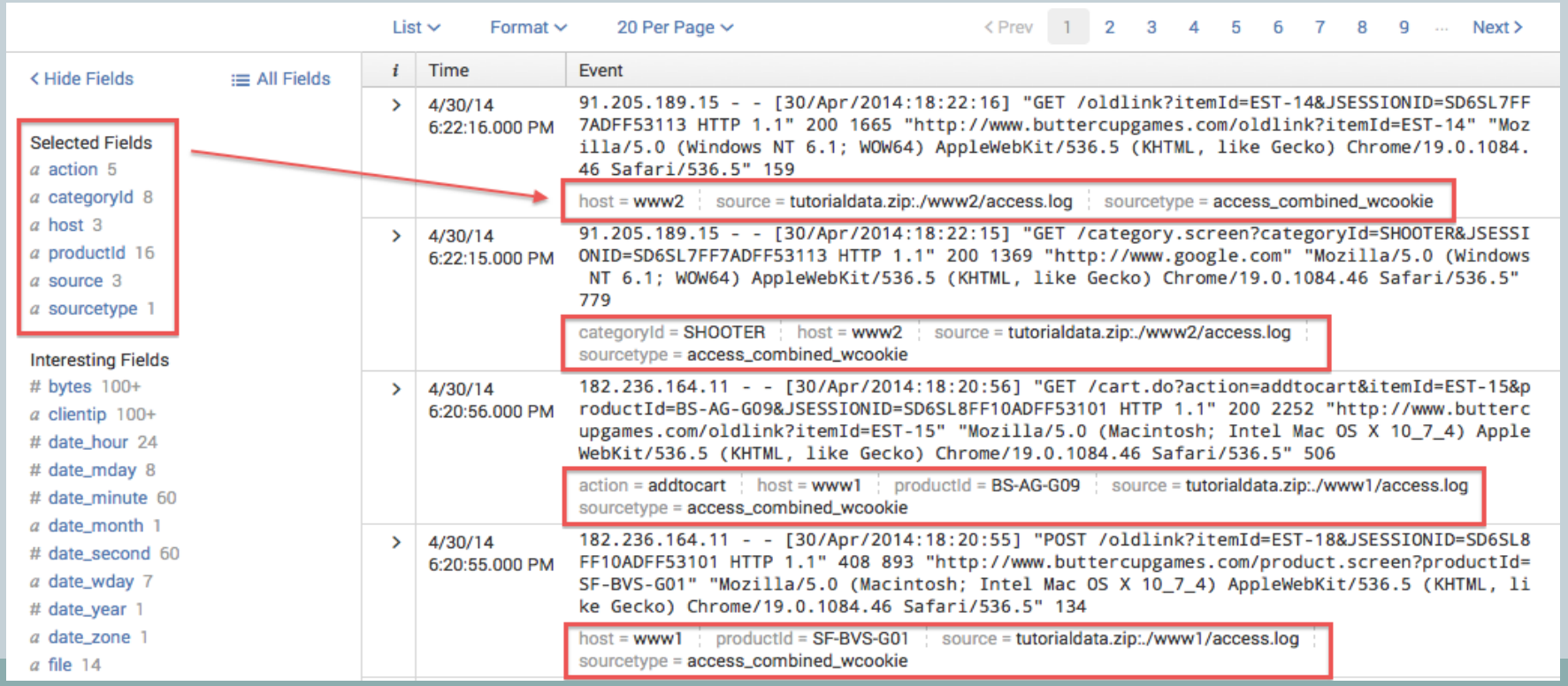
i	Time	Event
›	4/30/14 6:22:16.000 PM	91.205.189.15 - - [30/Apr/2014:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1665 "http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159 host = www2 source = tutorialdata.zip:./www2/access.log sourcetype = access_combined_wcookie
›	4/30/14 6:22:15.000 PM	91.205.189.15 - - [30/Apr/2014:18:22:15] "GET /category.screen?categoryId=SHOOTER&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1369 "http://www.google.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 779 host = www2 source = tutorialdata.zip:./www2/access.log sourcetype = access_combined_wcookie
›	4/30/14 6:20:56.000 PM	182.236.164.11 - - [30/Apr/2014:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "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" 506 host = www1 source = tutorialdata.zip:./www1/access.log sourcetype = access_combined_wcookie
›	4/30/14 6:20:55.000 PM	182.236.164.11 - - [30/Apr/2014:18:20:55] "POST /oldlink?itemId=EST-18&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 408 893 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "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" 134 host = www1 source = tutorialdata.zip:./www1/access.log sourcetype = access_combined_wcookie

KOENIG
step forward

Start Searching

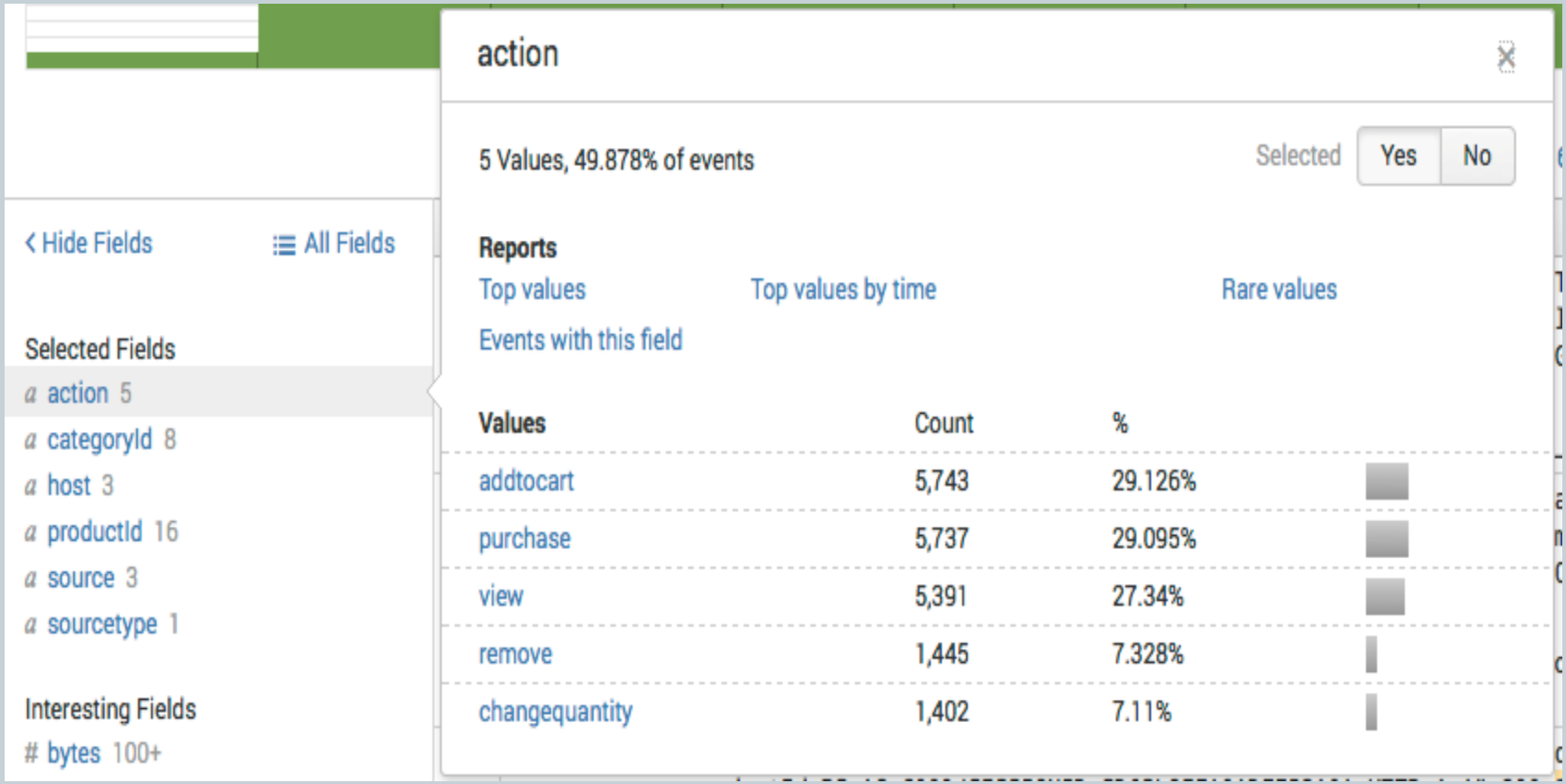
Select action, categoryId, and productId and close the Select Fields window.

The three fields appear under Selected Fields in the sidebar. The selected fields appear under the events in your search results if they exist in that particular event. Every event might not have the same fields.



Start Searching

- Under Selected Fields, click the action field.
  This opens the field summary for the action field.



KOENIG
step forward

Start Searching

- **Run more targeted searches**
- **Example1:** Search for successful purchases from the Buttercup Games store.

  sourcetype=access_* status=200 action=purchase

  You can search for failed purchases in a similar manner using status!=200, which looks for all events where the HTTP status code is not equal to 200.

  sourcetype=access_* status!=200 action=purchase

  Example 2: Search for general errors.

  (error OR fail* OR severe) OR (status=404 OR status=500 OR status=503)

  Example 3: Search for how many simulation games were bought yesterday.

  Select the Preset time range, Yesterday, from the time range picker and run:

  sourcetype=access_* status=200 action=purchase categoryId=simulation

KOENIG
step forward

Use The Search Language

- The searches you have run to this point have retrieved events from your Splunk index. You were limited to asking questions that could only be answered by the number of events returned.
- For example, we can run this search to see how many simulation games were purchased:
- sourcetype=access_* status=200 action=purchase categoryId=simulation

- To find this number for the days of the previous week, you have to run it against the data for each day of that week. To see which products are more popular than the other, you have to run the search for each of the eightcategoryId values and compare the results.

KOENIG
step forward

Use The Search Language

Learn with search assistant

Here we are going to talk about the search assistant to learn about the Splunk search processing language and construct searches.

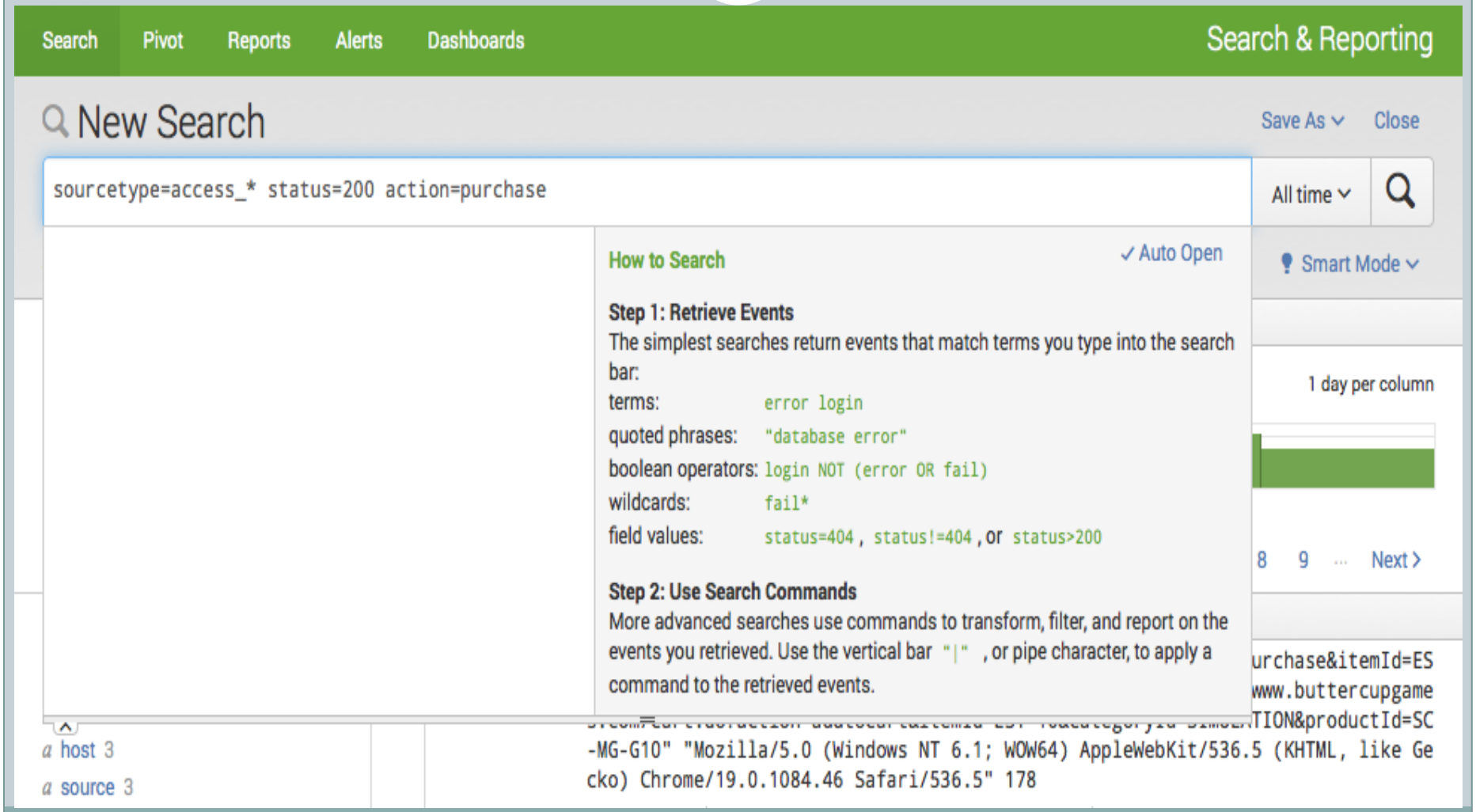
Return to the search dashboard and restrict your search to Yesterday:

sourcetype=access_* status=200 action=purchase

As you type in the search bar, search assistant opens with syntax and usage information for the search command (on the right side). If search assistant doesn't open, click the down arrow under the left side of the search bar. You've seen before that search assistant displays typeahead for keywords that you type into the search bar. It also explains briefly how to search.

KOENIG
step forward

Use The Search Language



KOENIG
step forward

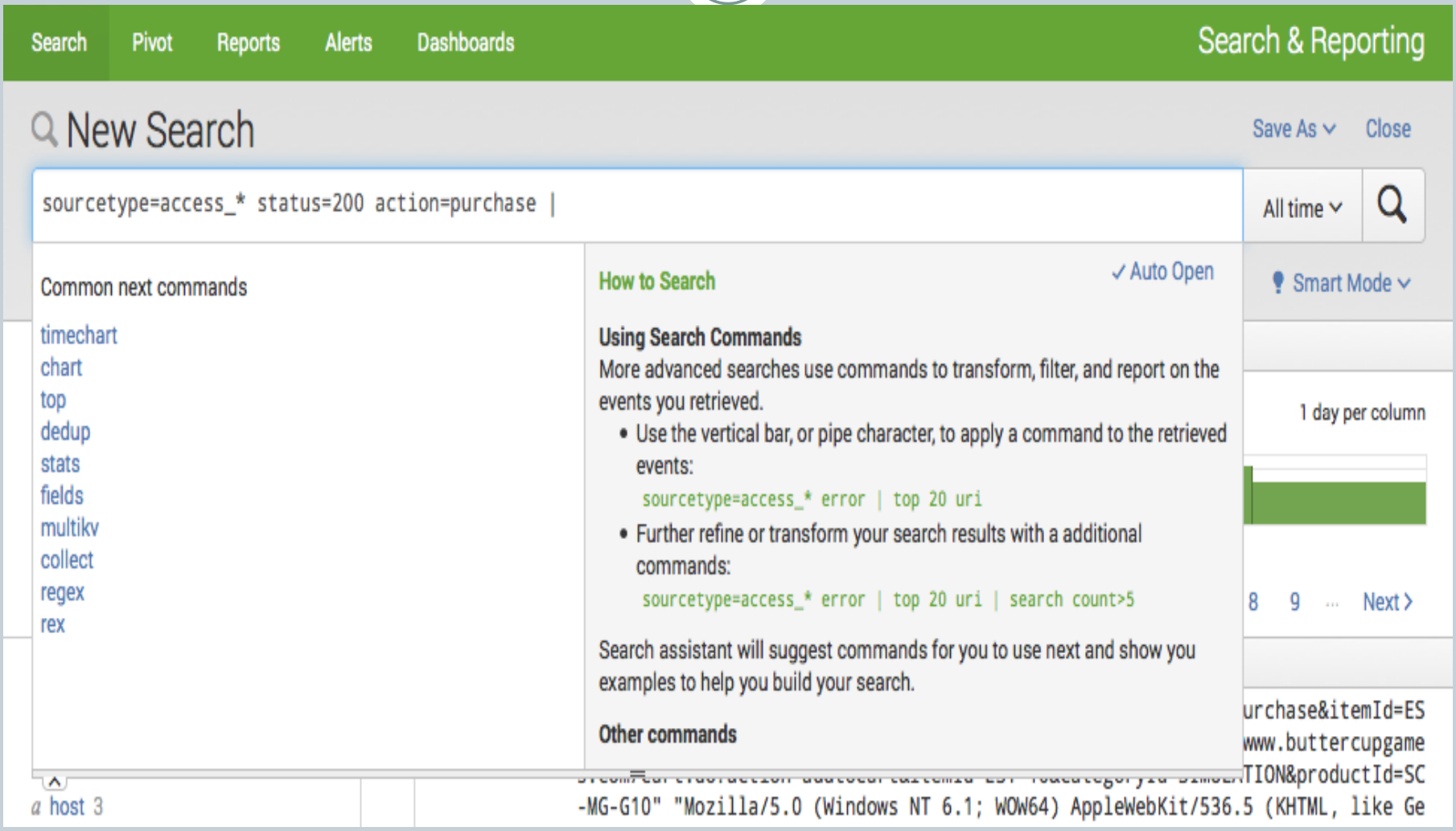
Use The Search Language

Type a pipe character, " | ", into the search bar.

The pipe indicates to Splunk that you're about to use a command, and that you want to use the results of the search to the left of the pipe as the input to this command. You can pass the results of one command into another command in a series, or pipeline, of search commands.

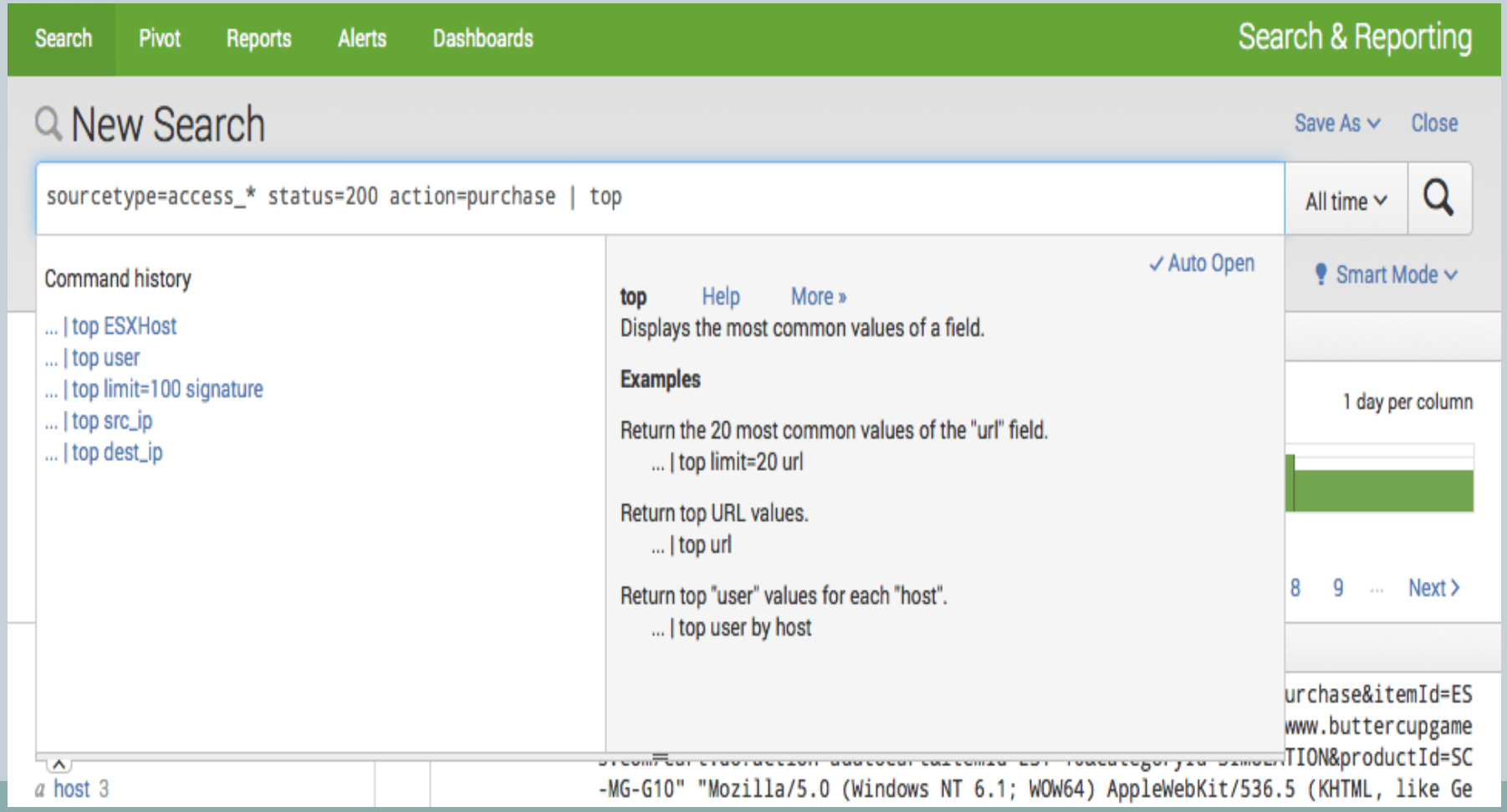
KOENIG
step forward

Use The Search Language



Use The Search Language

You want Splunk to give you the most popular items bought at the online store.



KOENIG
step forward

Use The Search Language

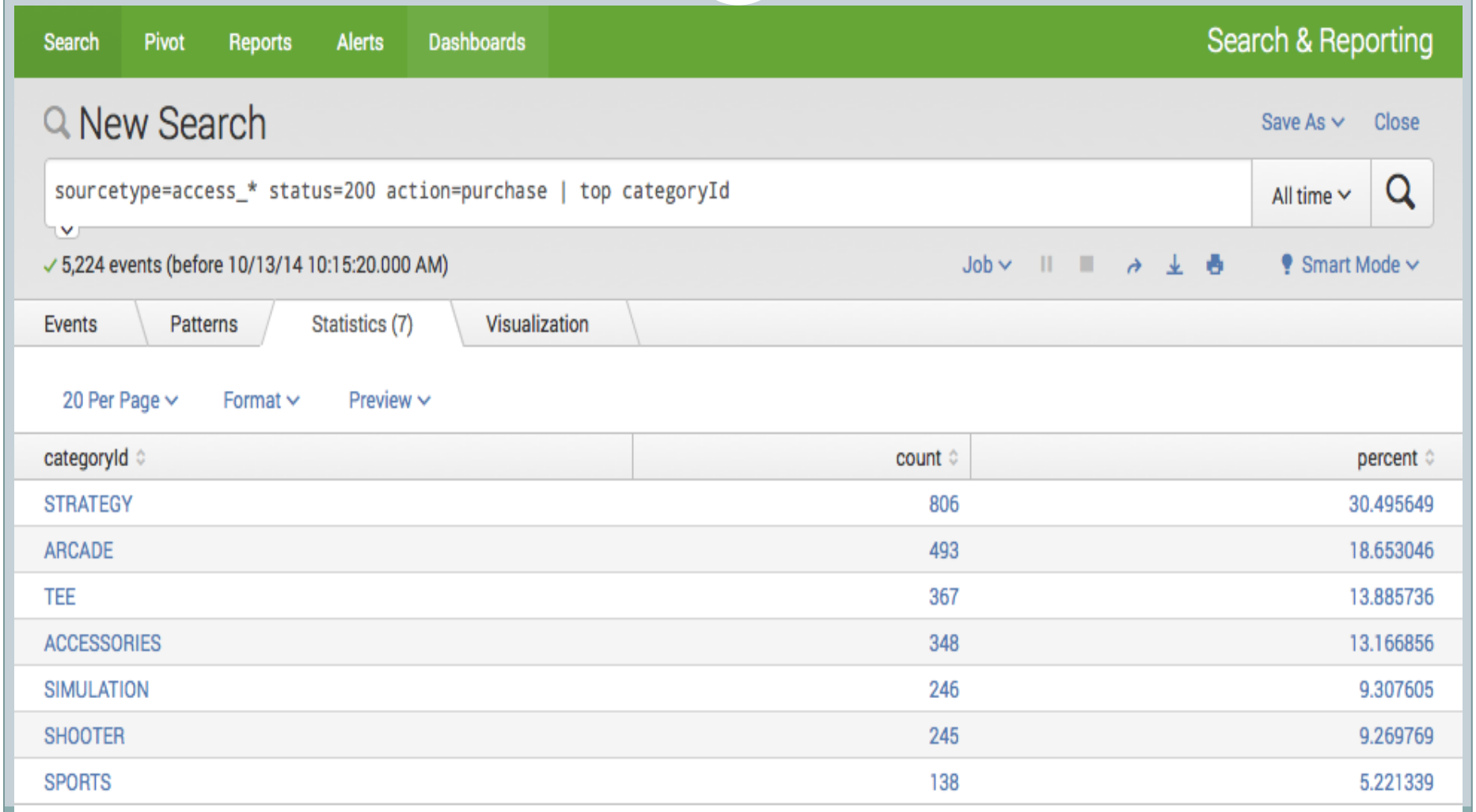
- Type the categoryId field into the search bar to complete your search.
  sourcetype=access_* status=200 action=purchase | top categoryId

- **View reports in the Statistics tab**

  The results of a search are reports. The top command is a transforming command and returns a tabulated report for the most common values of categoryId. You can view the results of transforming searches in the Statistics tab.

KOENIG
step forward

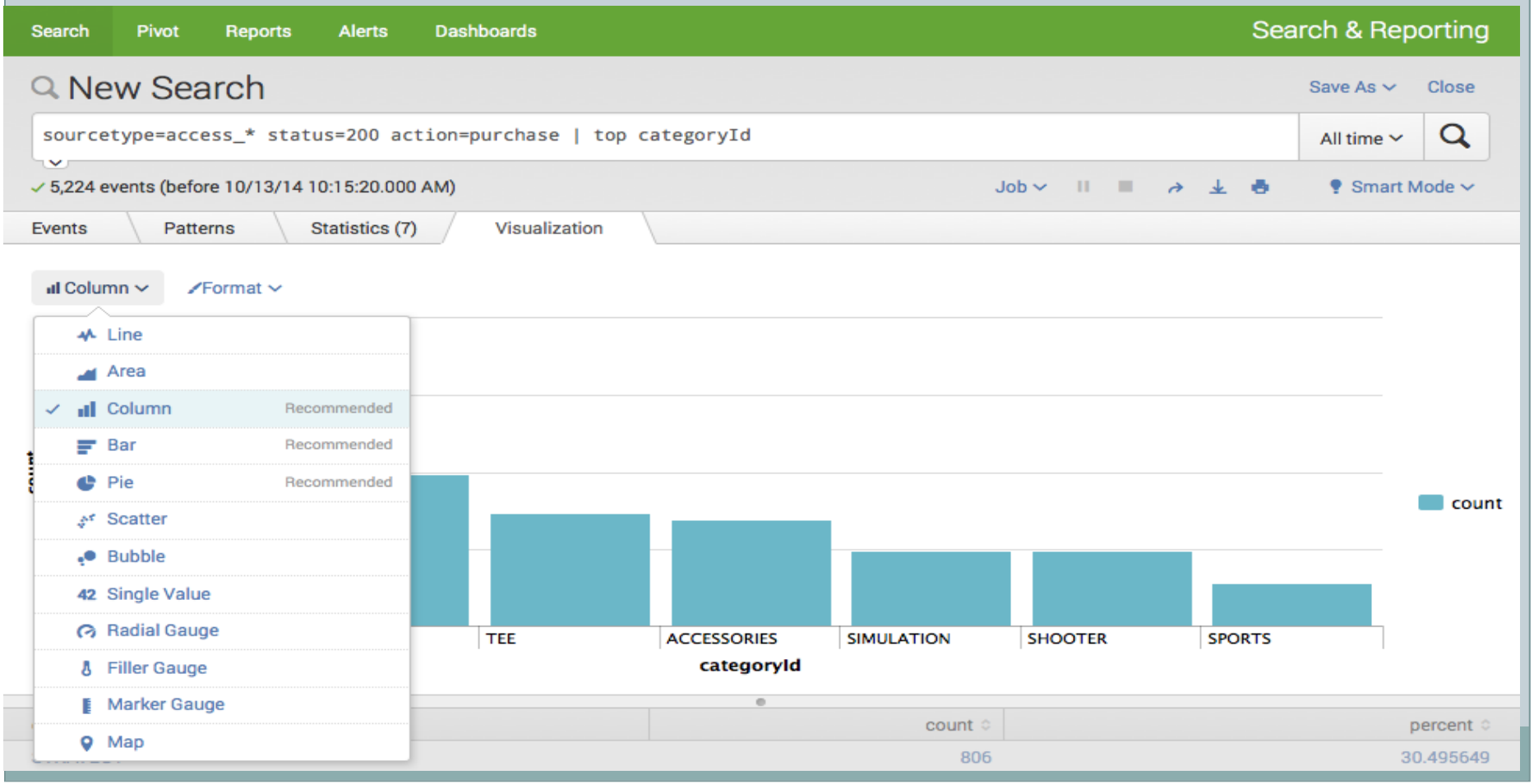
Use The Search Language



Use The Search Language

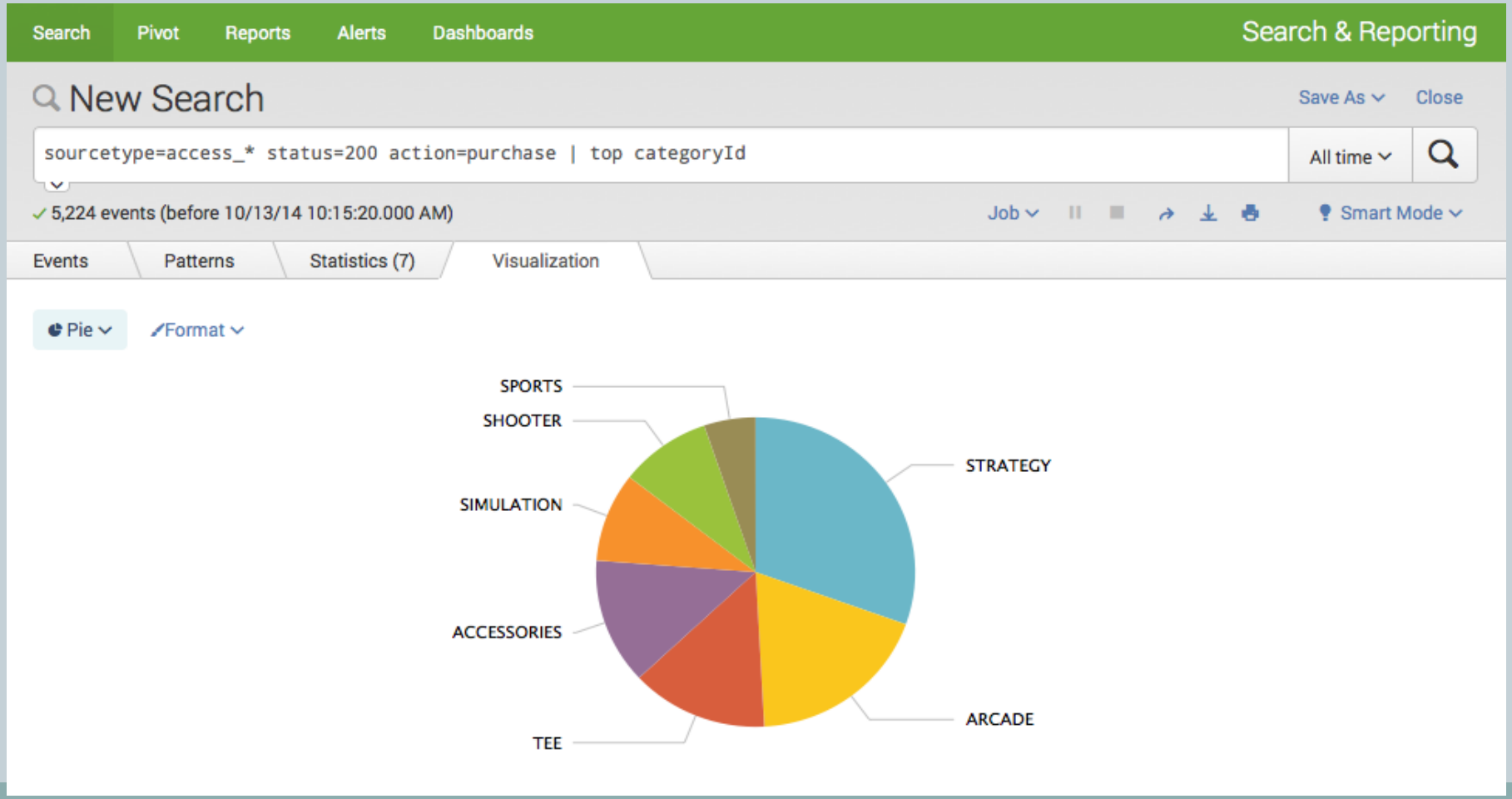
- View and format reports in the Visualization tab

  You can also view the results of transforming searches in the Visualizations tab



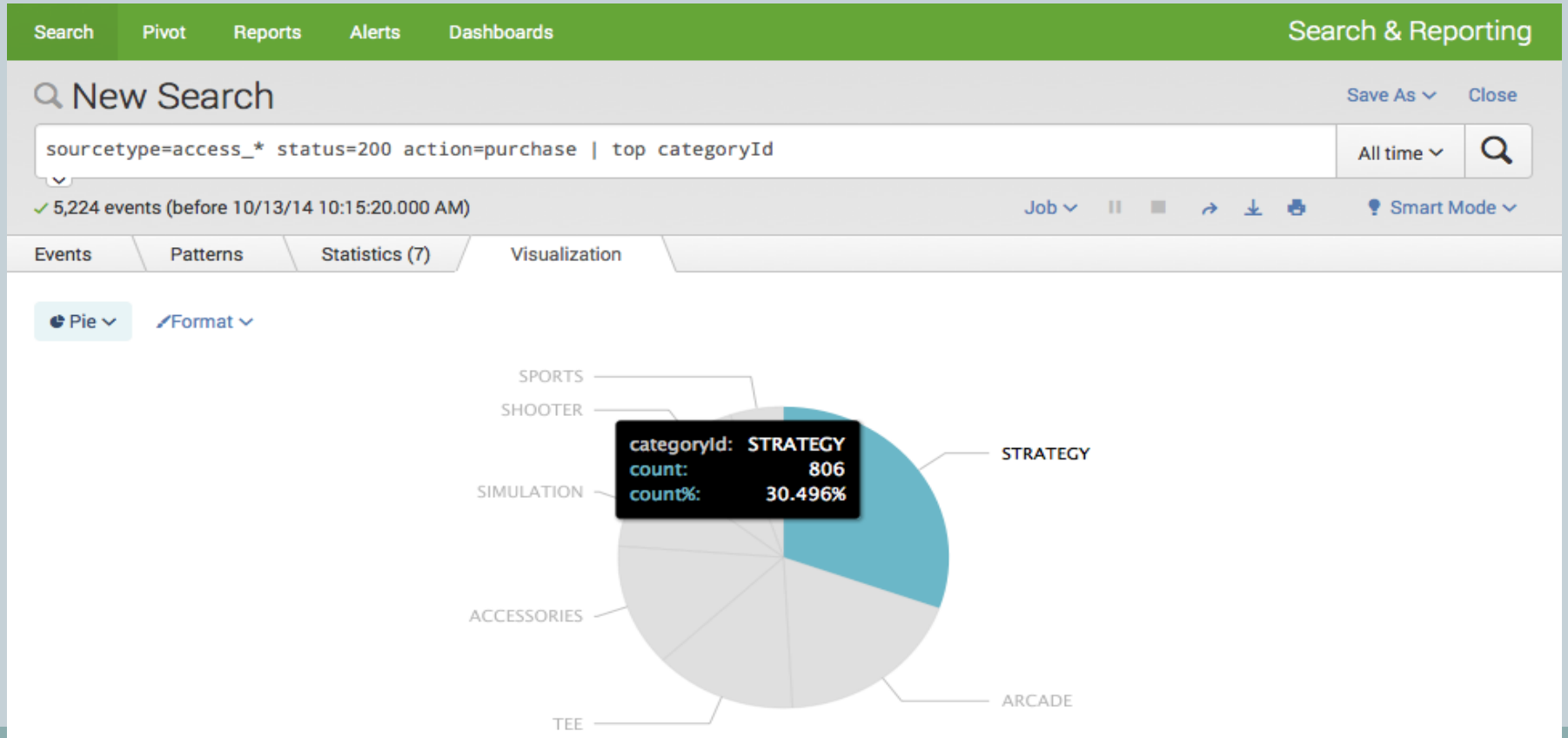
Use The Search Language

SELECT PIE



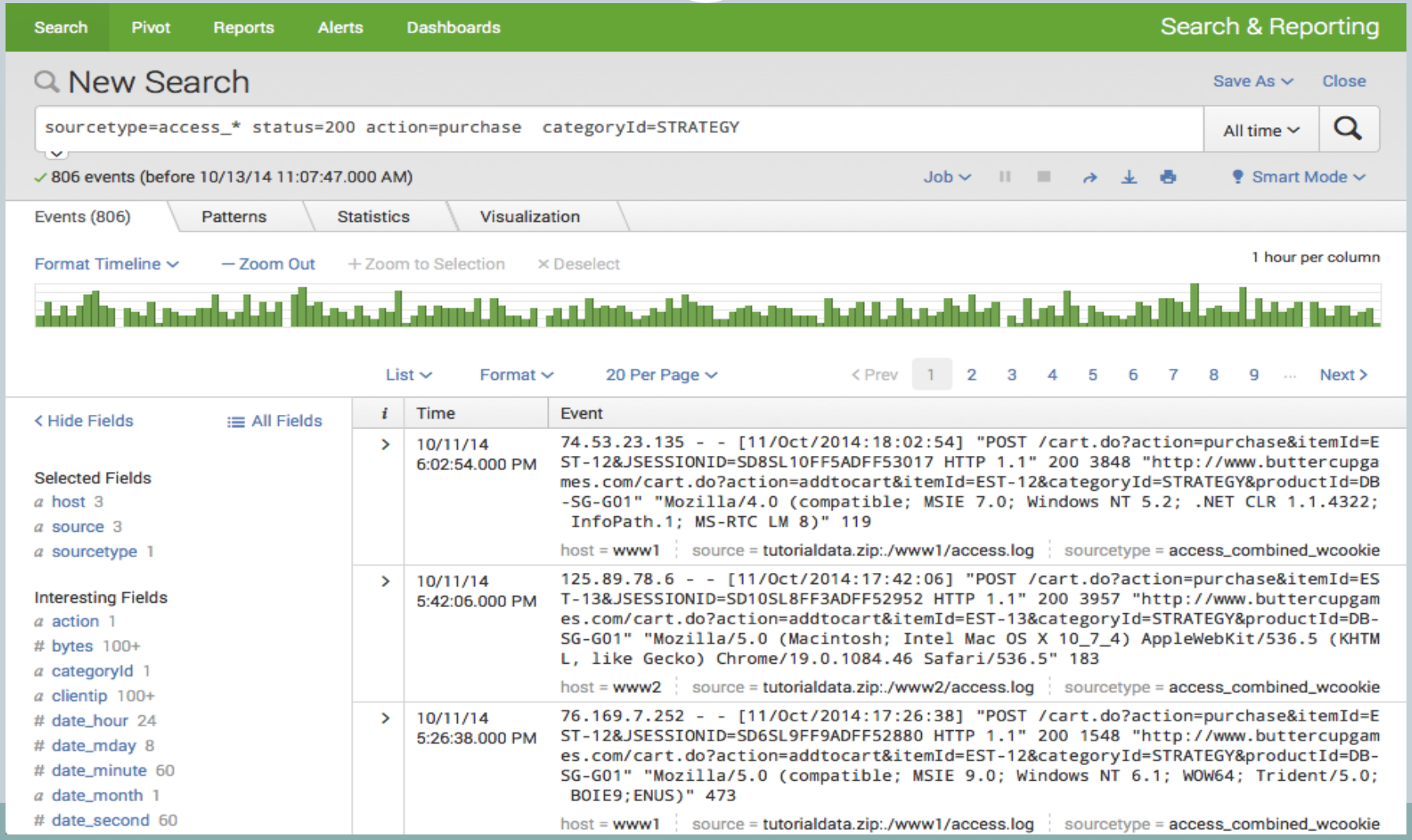
Use The Search Language

Mouse over each slice of the pie to see the count and percentage values for each categoryId.



KOENIG
step forward

Use The Search Language



KOENIG
step forward

Use a Subsearch

- This topic walks you through examples of correlating events with subsearches.

  A subsearch is a search with a search pipeline as an argument. Subsearches are contained in square brackets and evaluated first. The result of the subsearch is then used as an argument to the primary, or outer, search.

  Example 1: Without a subsearch

  Let's try to find the single most frequent shopper on the Buttercup Games online store and what this customer has purchased.

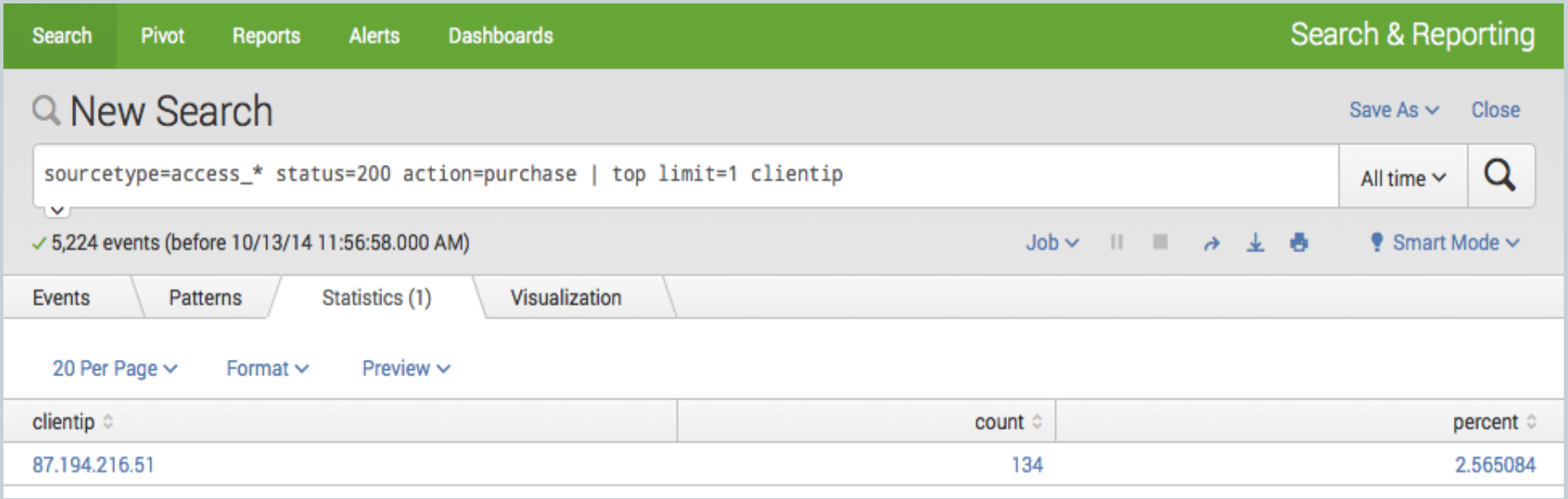
  To do this, search for the customer who accessed the online shop the most.

  1. Use the top command:

  sourcetype=access_* status=200 action=purchase | top limit=1 clientip

  Limit the top command to return only one result for the clientip. To see more than one "top purchasing customer", change this limit value.

Use a Subsearch

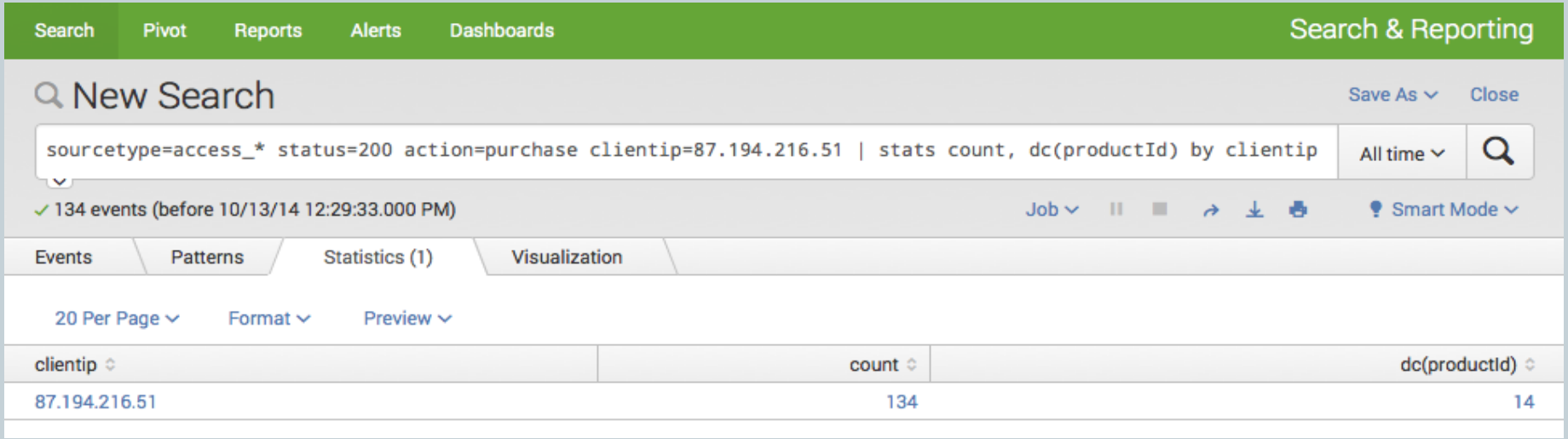


This search returns one clientip value, which we'll use to identify our VIP customer.

Use a Subsearch

Use the stats command to count this VIP customer's purchases:

sourcetype=access_* status=200 action=purchase clientip=87.194.216.51 | stats count, dc(productId) by clientip



This search used the count( ) function which only returns the total count of purchases for the customer. The dc( ) function is used to count how many different products he buys.

KOENIG
step forward

Use a Subsearch

The drawback to this approach is that you have to run two searches each time you want to build this table. The top purchaser is not likely to be the same person at any given time range.

Hence we induce the concept of SUBSEARCH !!

KOENIG
step forward

Use a Subsearch

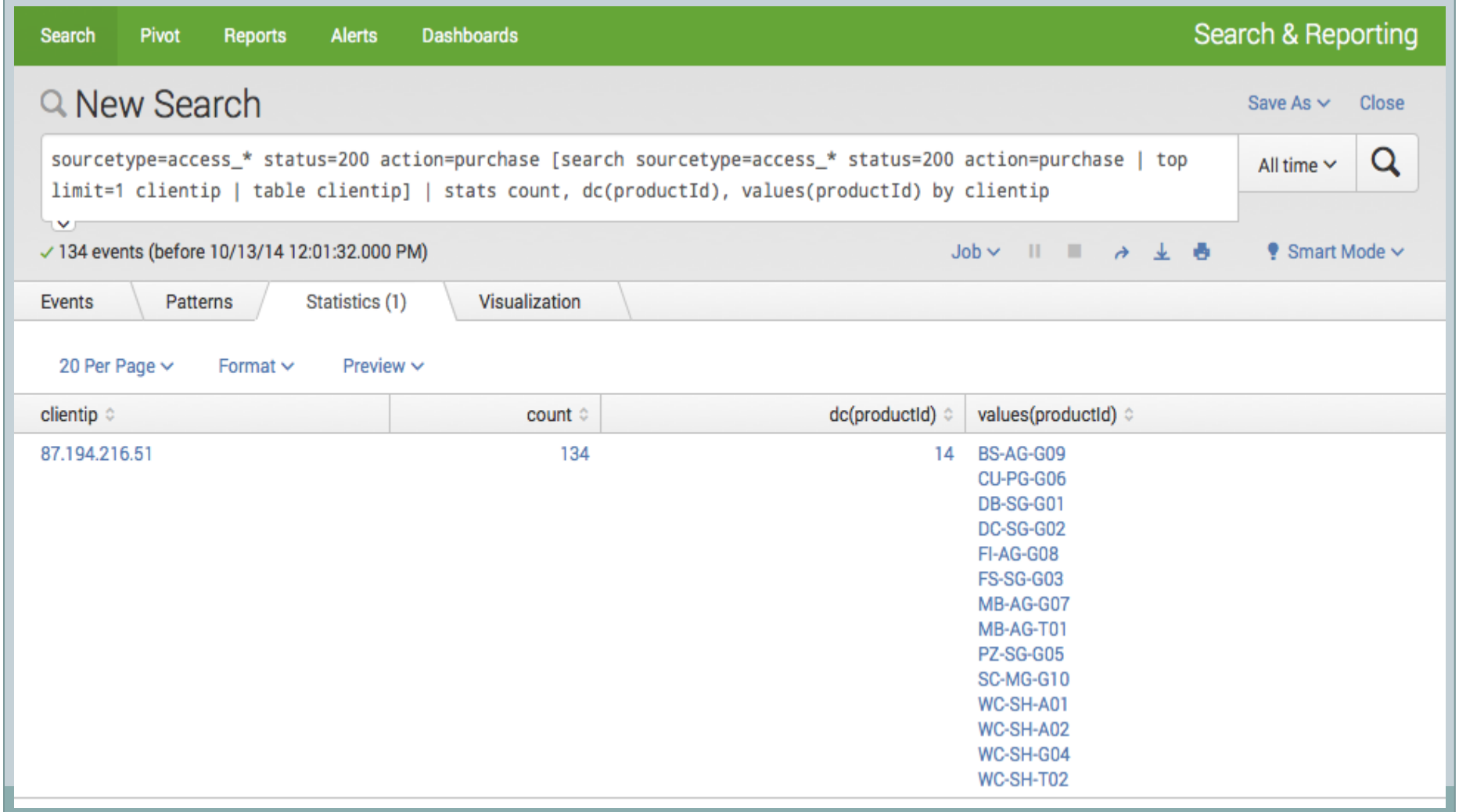
Example 2: With a subsearch

```
sourcetype=access_* status=200 action=purchase [search
sourcetype=access_* status=200 action=purchase | top limit=1 clientip | table
clientip] | stats count, dc(productId), values(productId) by clientip
```

- Here, the subsearch is the segment that is enclosed in square brackets, []. This search, search sourcetype=access_* status=200 action=purchase | top limit=1 clientip | table clientip is the same as Example 1 Step 1, except for the last piped command, | table clientip
- Because the top command returns count and percent fields as well, the table command is used to keep only the clientip value.

KOENIG
step forward

Use a Subsearch



KOENIG
step forward

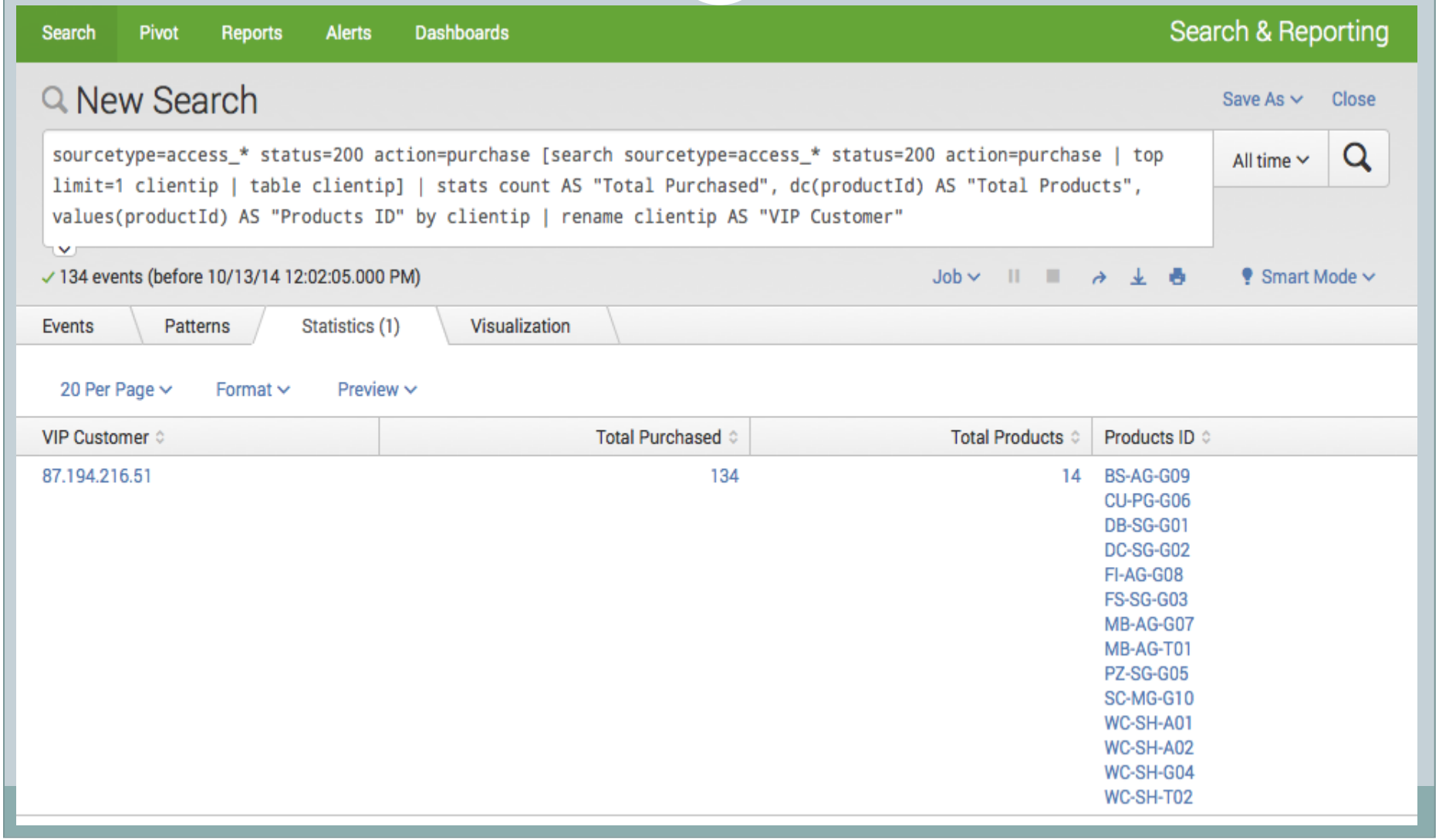
Use a Subsearch

Rename the columns to make the information more understandable.

```
sourcetype=access_* status=200 action=purchase [search
sourcetype=access_* status=200 action=purchase | top limit=1 clientip | table
clientip] | stats count AS "Total Purchased", dc(productId) AS "Total Products",
values(productId) AS "Products ID" by clientip | rename clientip AS "VIP
Customer"
```

KOENIG
step forward

Use a Subsearch



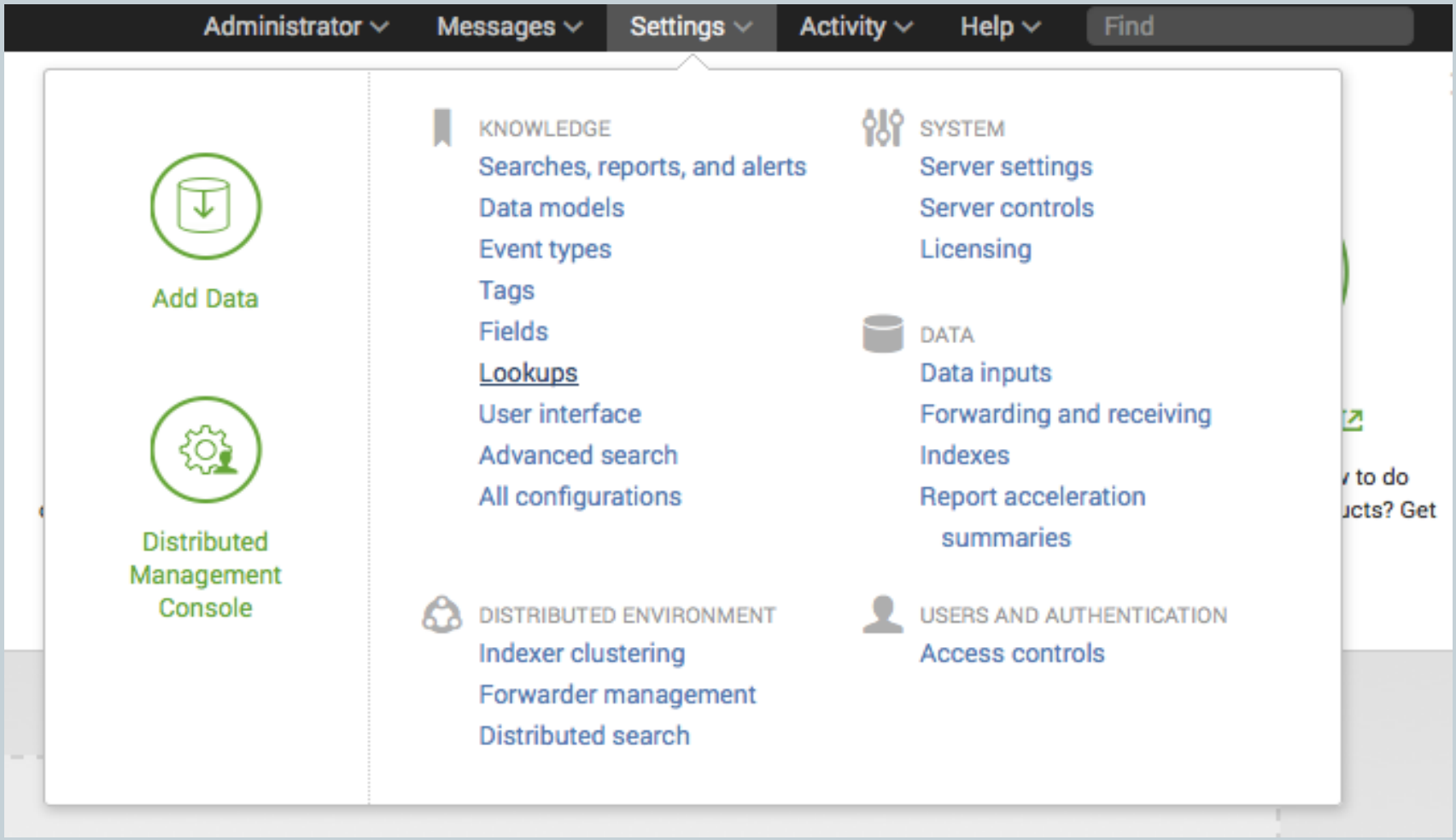
KOENIG
step forward

Use Field Lookups

This topic takes you through using field lookups to add new fields to your events. Field lookups let you reference fields in an external CSV file that match fields in your event data. Using this match, you can enrich your event data by adding more meaningful information and searchable fields to each event.

KOENIG
step forward

Use Field Lookups



KOENIG
step forward

Use Field Lookups

Lookups

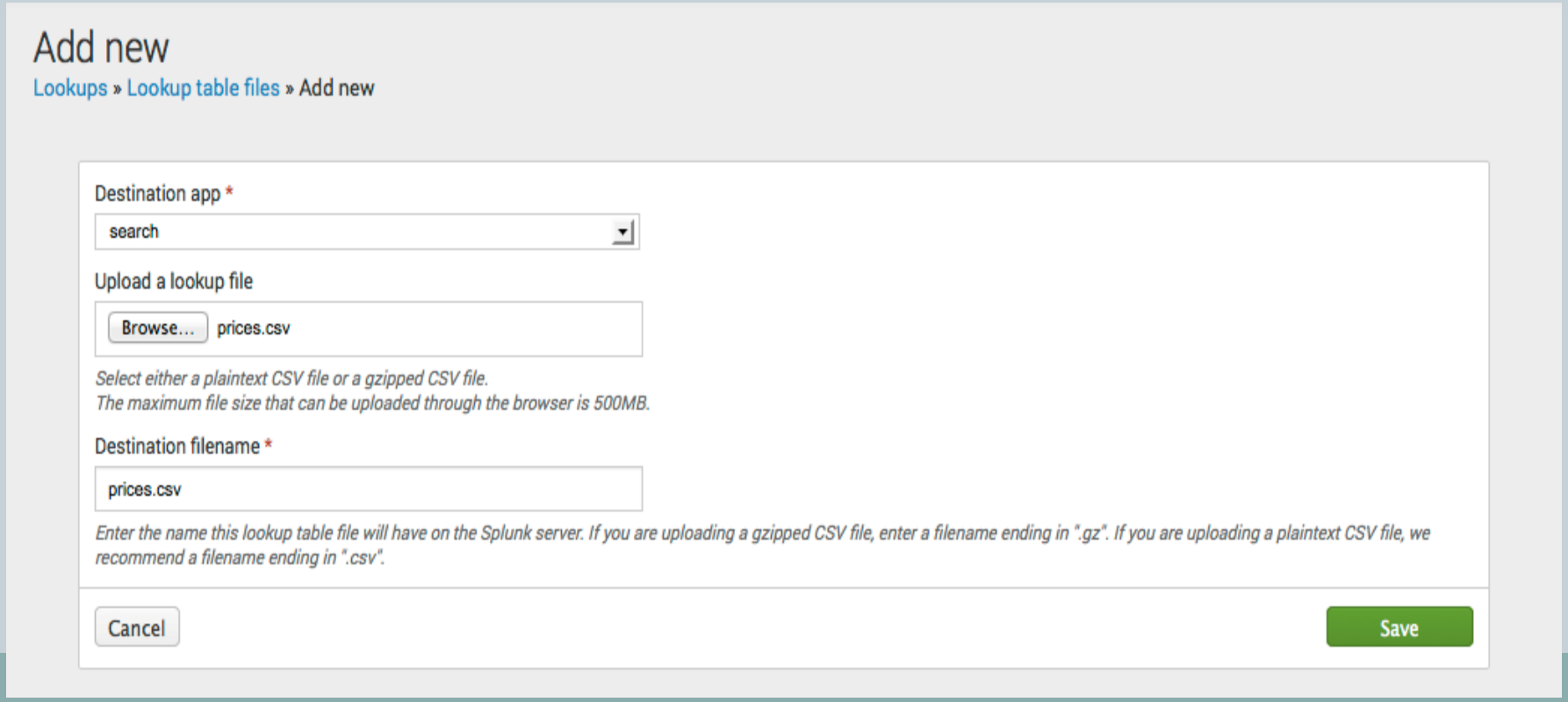
Create and configure lookups.

	Actions
Lookup table files *List existing lookup tables or upload a new file.*	Add new
Lookup definitions *Edit existing lookup definitions or define a new file-based or external lookup.*	Add new
Automatic lookups *Edit existing automatic lookups or configure a new lookup to run automatically.*	Add new

Use Field Lookups

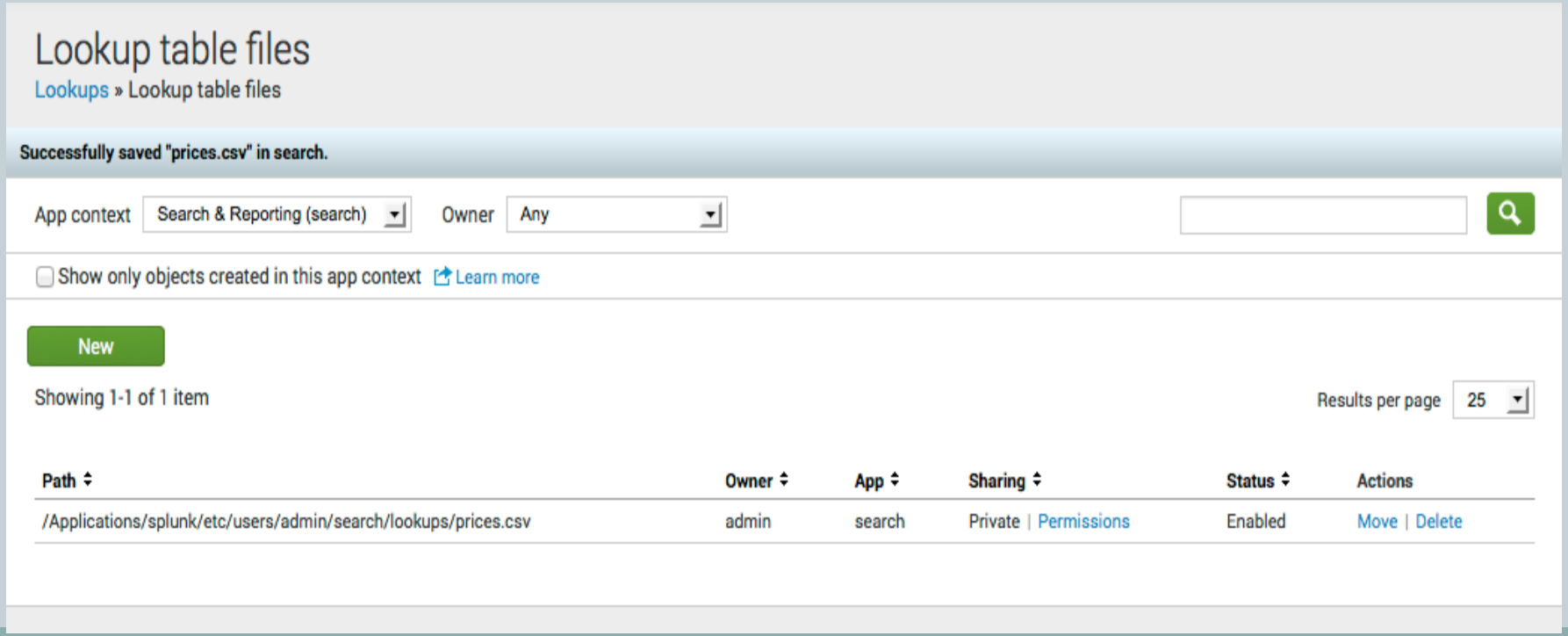
- Upload the lookup table file

1. In the Lookups manager under "Actions" for Lookup table files, click Add new.
   This takes you to the Add new' lookup table files view where you upload CSV files to use in your definitions for field lookups.



Use Field Lookups

2. To save your lookup table file in the Search app, leave the Destination app as search.
3. Under Upload a lookup file, browse for the CSV file (prices.csv) to upload.
4. Save



Use Field Lookups

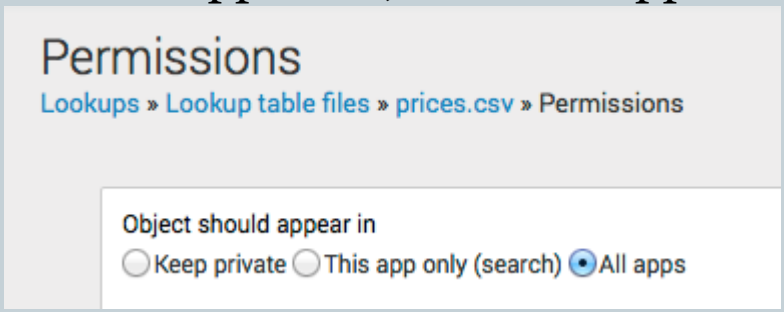
- **Share the lookup table file globally**

  If the lookup file is not shared, you can not select it when you define the lookup.

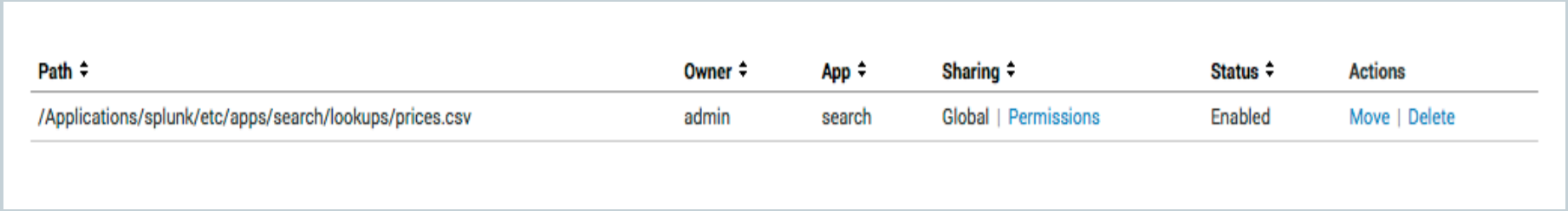
  1. Go to the Lookup table files list.
  2. Under Sharing for the prices.csv lookup table's Path, click Permissions.

  This opens the Permission dialog box for the prices.csv lookup file.

  3. Under Object should appear in, select All apps.



  4. Click Save.



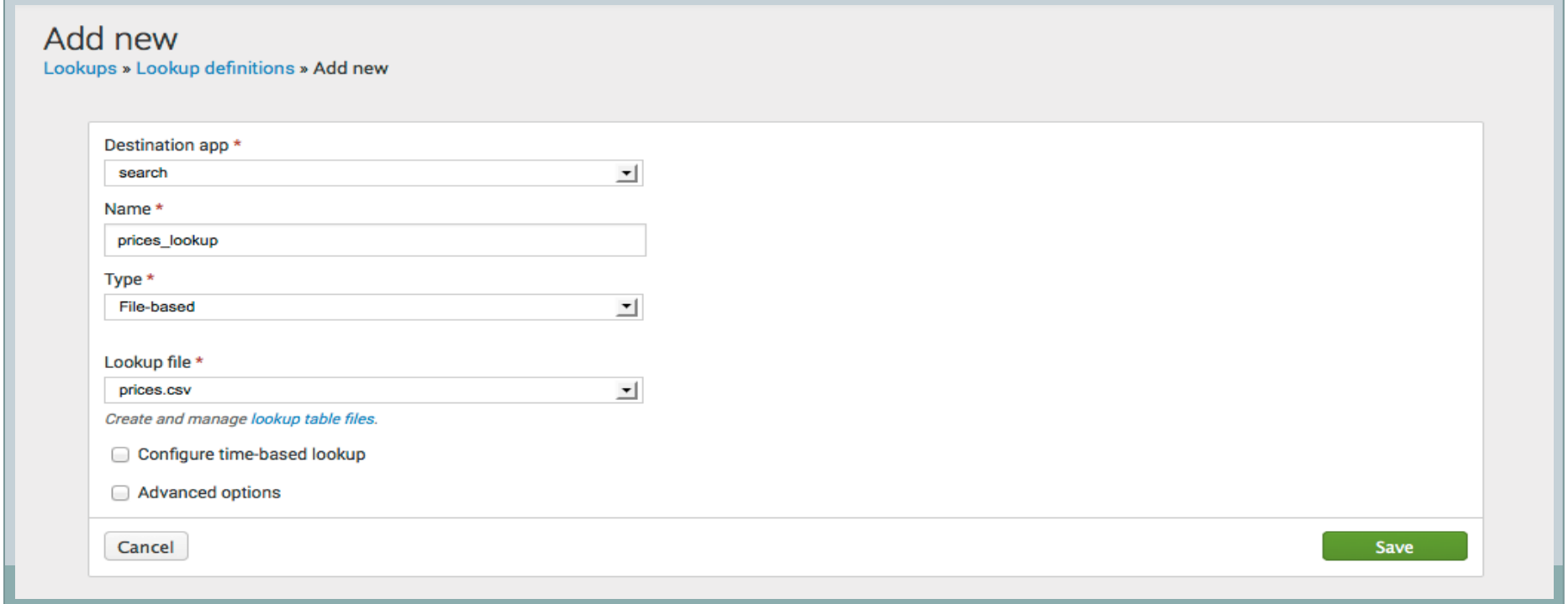
Path	Owner	App	Sharing	Status	Actions
/Applications/splunk/etc/apps/search/lookups/prices.csv	admin	search	Global | Permissions	Enabled	Move | Delete

Use Field Lookups

- **Add the field lookup definitionAdd the field lookup definition**

  1. Return to the Lookups manager.
  2. Under Actions for Lookup definitions, click Add New.

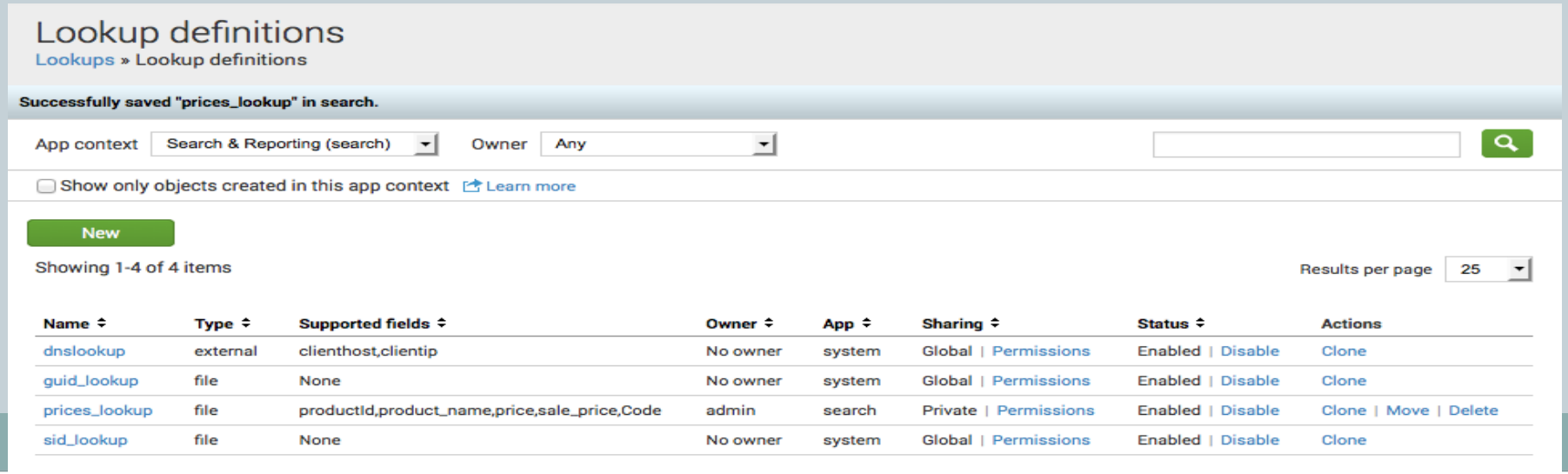
  This takes you to the Add new lookups definitions view where you define your field lookup.



Use Field Lookups

3. Leave the Destination app as search.
4. Name your lookup prices_lookup.
5. Under Type, select File-based.
   - File-based lookups add fields from a static table, usually a CSV file.
6. Under Lookup file, select prices.csv (the name of your lookup table).
7. Leave Configure time-based lookup and Advanced options unselected.
8. Click Save.

   This defines prices_lookup as a file-based lookup.



Use Field Lookups

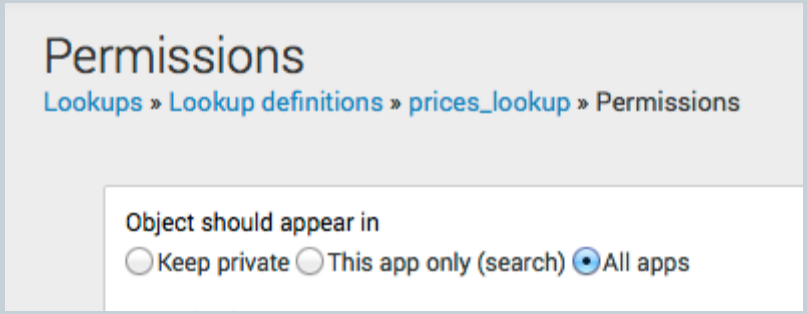
- Share the lookup definition with all apps

  1. Return to the Lookup definitions list.
  2. Under Sharing for prices_lookup, click Permissions.

  The Permission dialog box for the prices.lookup opens.

  3. Under Object should appear in, select All apps.
  4. Click Save.

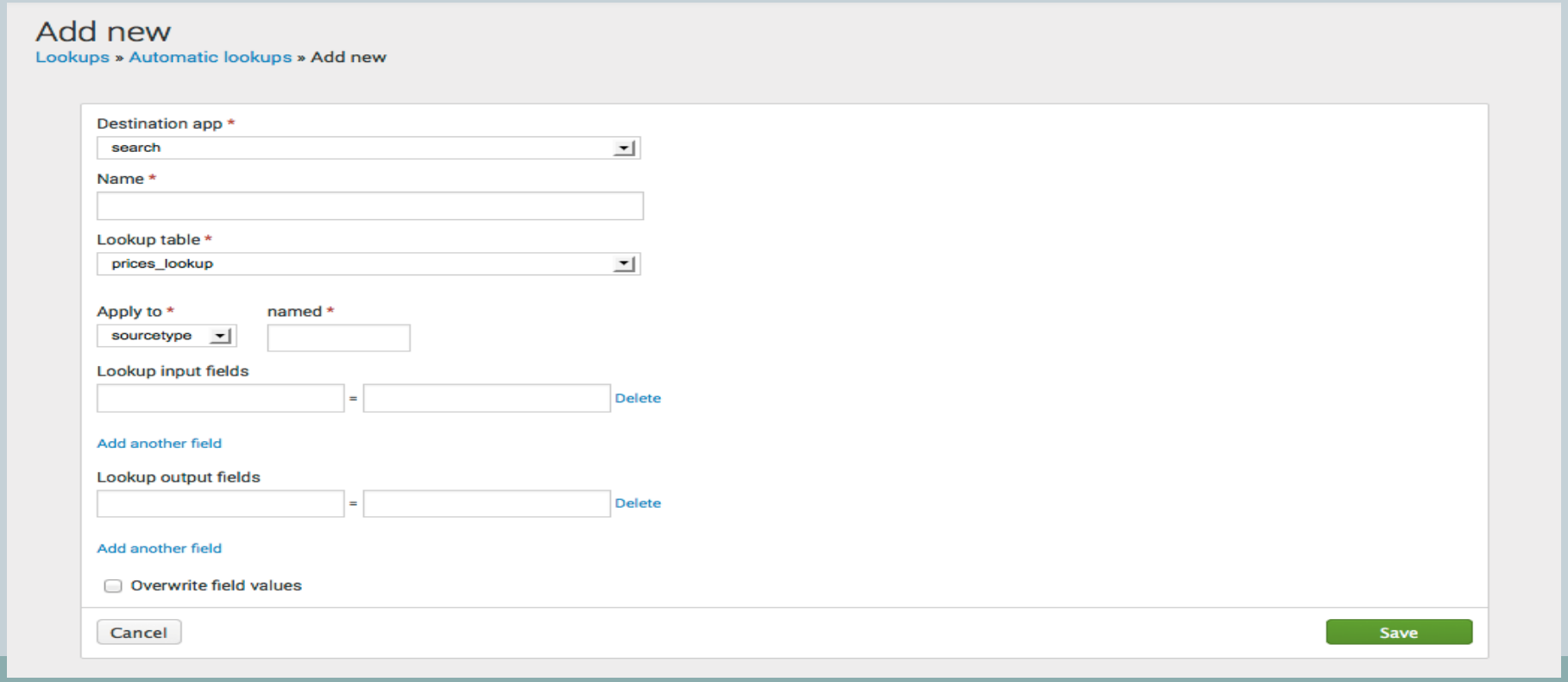
  Now, prices_lookup should be shared with Global permissions.



Use Field Lookups

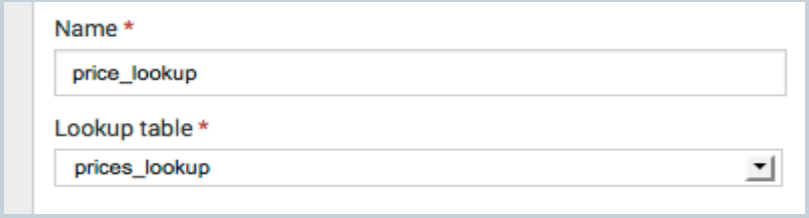
- **Make the lookup automatic**

  1. In the Lookups manager, under Actions for Automatic lookups, click Add New. This takes you to the Add New automatic lookups view where you configure the lookup to run automatically.

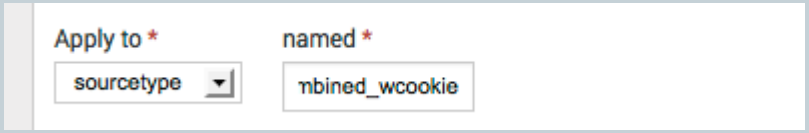


Use Field Lookups

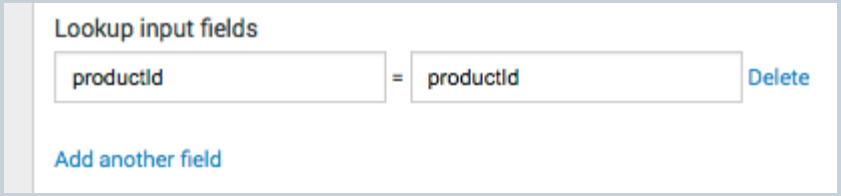
2. Leave the Destination app as search.
3. Name your automatic lookup price_lookup.
4. Under Lookup table, select prices_lookup.



5. Under Apply to and named, select sourcetype and type in access_combined_wcookie.



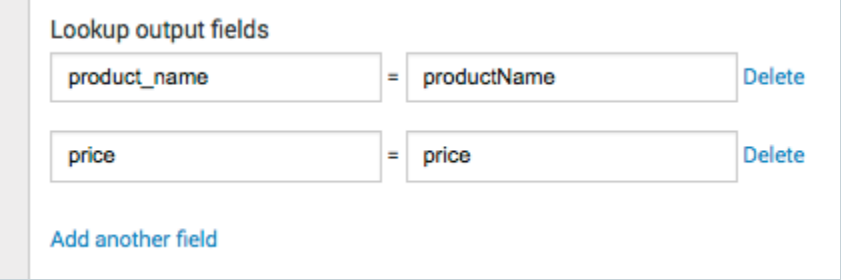
6. Under Lookup input fields type in productId in both text areas under Lookup input fields .



Splunk Enterprise matches the field in the lookup table (which is the one specified on the left) with the field on the right (which is the field in your events). In this case the field names match.

Use Field Lookups

7. Under Lookup output fields, type in the name of the fields that you want to add to your event data based on the input field matching and rename the fields.



7.1 In the first text area, type product_name, which contains the descriptive name for each productId.

7.2. In the second text area, after the equal sign, type productName. This renames the field to productName.

7.3. Click Add another field to add more fields after the first one.

7.4. Add the field price, which contains the price for each productId. Do not rename this field.

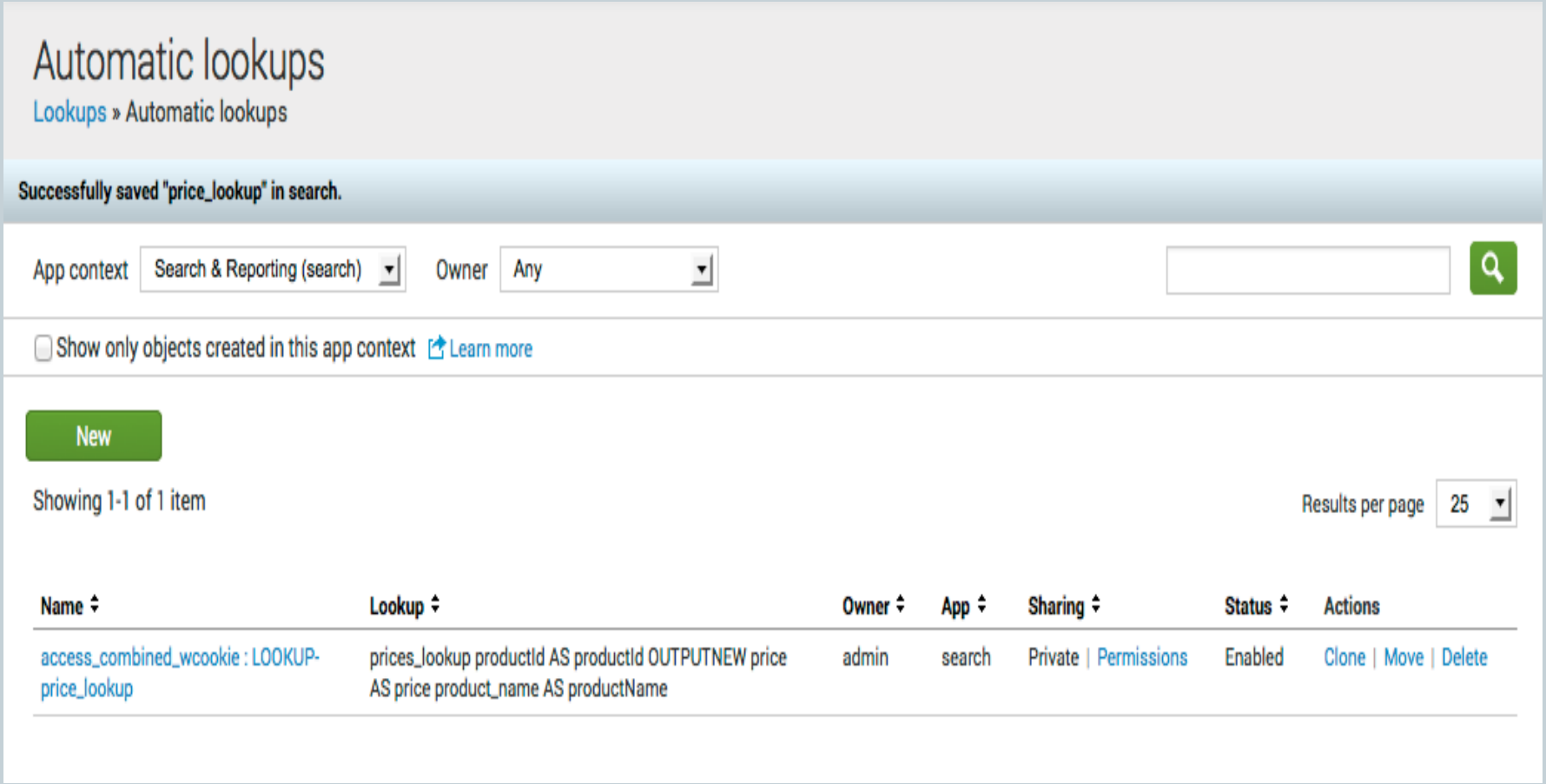
8. Leave Overwrite field values unchecked.

9. Click Save.

KOENIG
step forward

Use Field Lookups

This returns you to the list of automatic lookups and you should see your configured lookup.



Use Field Lookups

- Show the new fields in your search results

  1. Return to Search.
  2. Run the search for web access activity.

  sourcetype=access_*

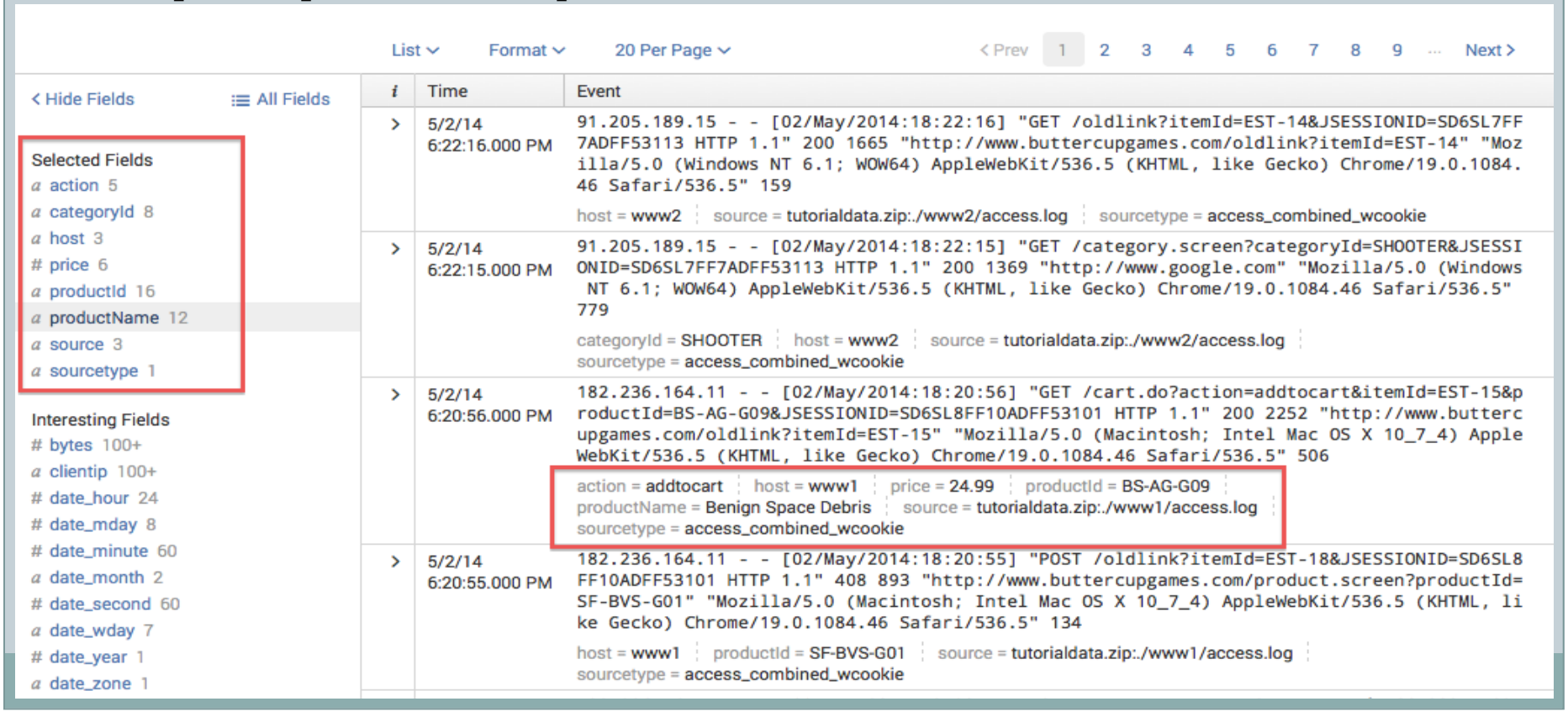
  3. Scroll through the list of Interesting Fields in the fields sidebar, and find the price field.
  4. Click price to open its field summary dialog box.

Use Field Lookups

5. Next to Selected, click Yes.
6. Close the dialog box.

The price field appears under Selected Fields in the fields sidebar.

7. Repeat Steps 3 to 5 for the productName field.



Use Field Lookups

Search with the new lookup fields

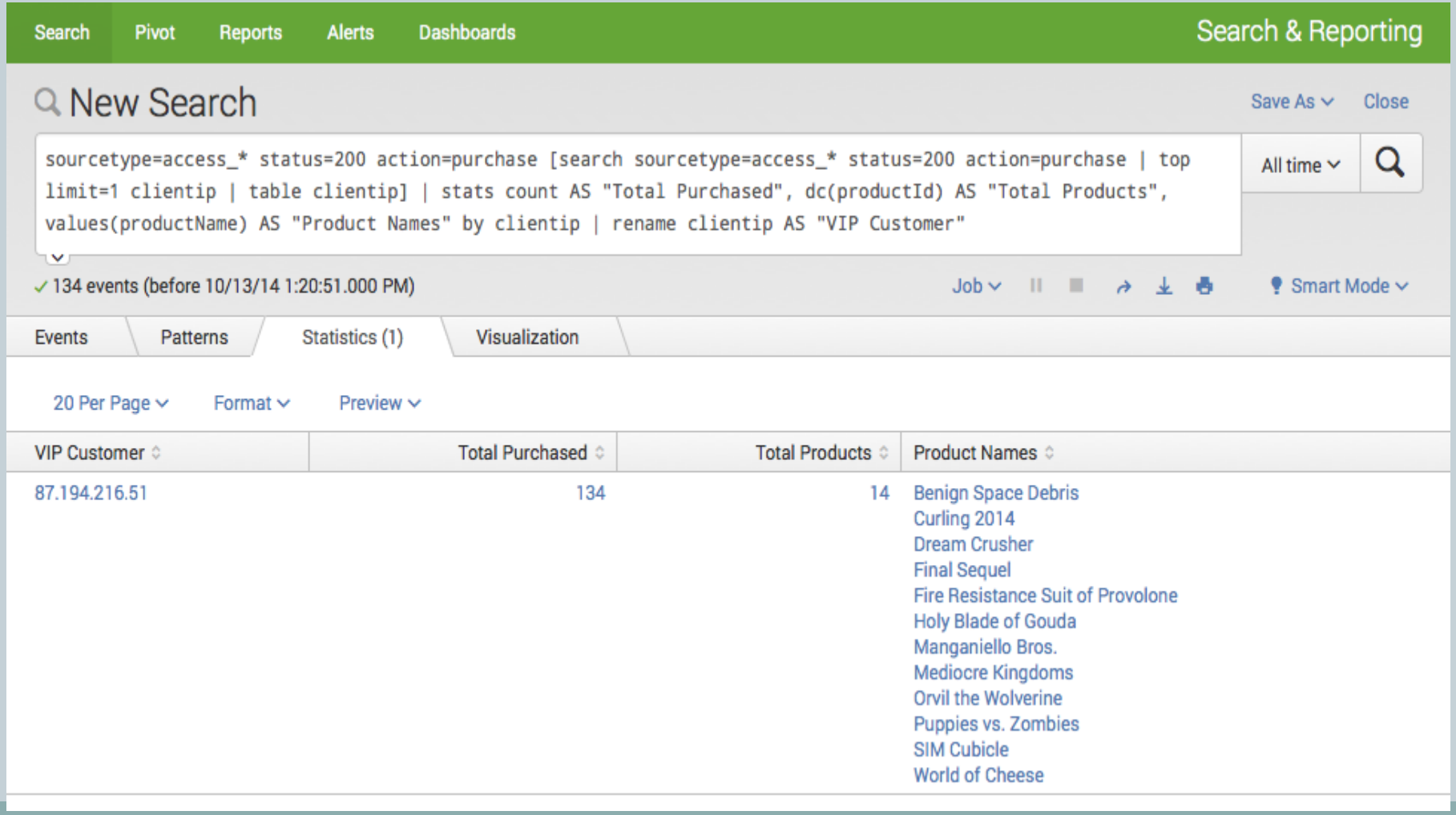
- 1. Copy and paste or type in the previous subsearch example to see what the VIP customer bought. This time, replace the productId field with productName.

  sourcetype=access_* status=200 action=purchase [search sourcetype=access_* status=200 action=purchase | top limit=1 clientip | table clientip] | stats count AS "Total Purchased", dc(productId) AS "Total Products", values(productName) AS "Product Names" by clientip | rename clientip AS "VIP Customer"

The result is the same as in the previous subsearch example, except that the VIP customer's purchases are more meaningful with the added descriptive product names.

KOENIG
step forward

Use Field Lookups



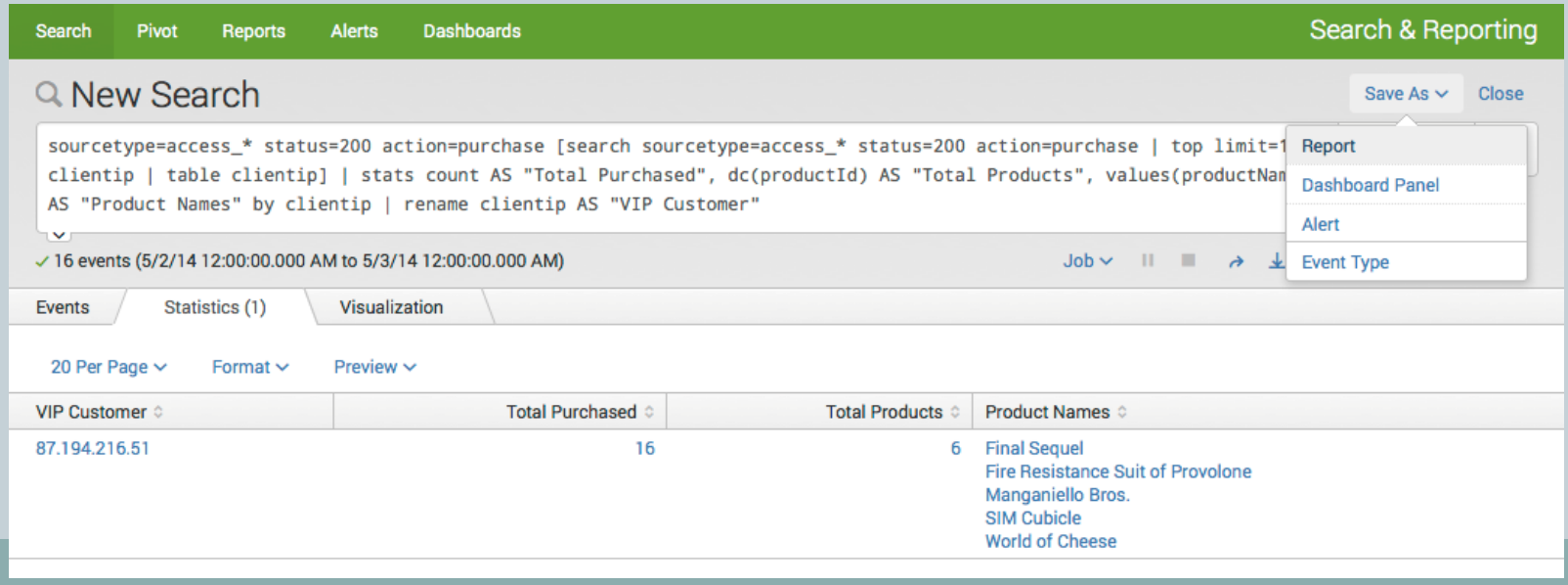
Saving and Sharing Reports

- Save as a report

  1. Select the time range Yesterday and run the subsearch

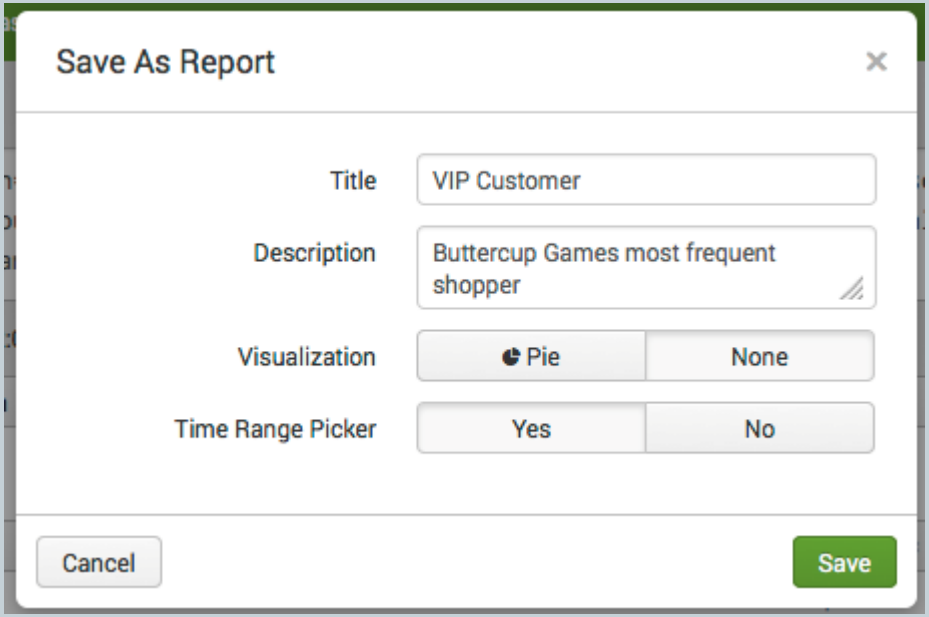
  sourcetype=access_* status=200 action=purchase [search sourcetype=access_* status=200 action=purchase | top limit=1 clientip | table clientip] | stats count AS "Total Purchased", dc(productId) AS "Total Products", values(productName) AS "Product Names" by clientip | rename clientip AS "VIP Customer"

  2. To save it as a report, click Save as above the search bar and select Report.



Saving and Sharing Reports

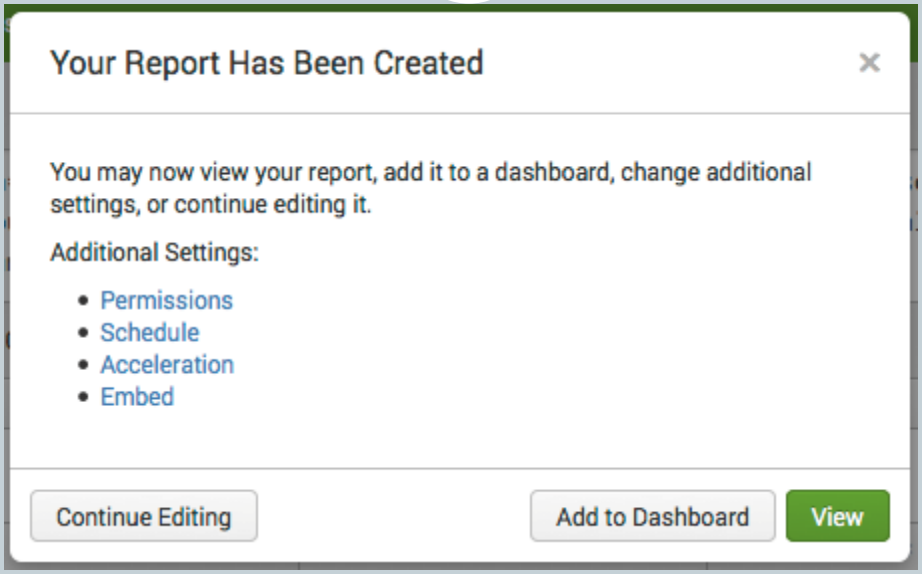
3. Enter a Title VIP Customer.
4. (Optional) Enter a Description Buttercup Games most frequent shopper.



5. Because the report is a table, for Visualization, click None.
6. To include a Time Range Picker, click Yes.
7. Click Save.

The Your report has been created dialog box opens.

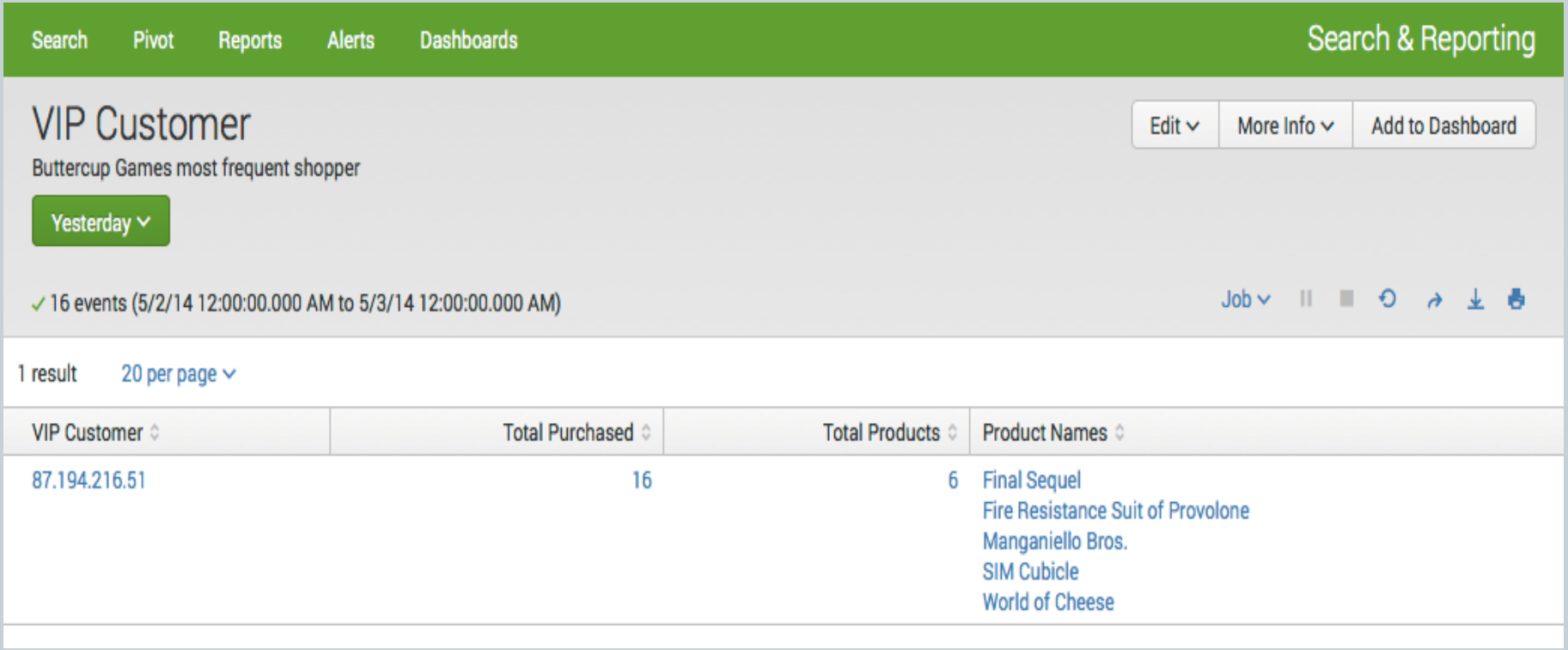
Saving and Sharing Reports



- There are other options in this window.
  Continue Editing lets you refine the search and report format.
  Add to dashboard lets you add the report to a new or existing dashboard.
  View lets you view the report.

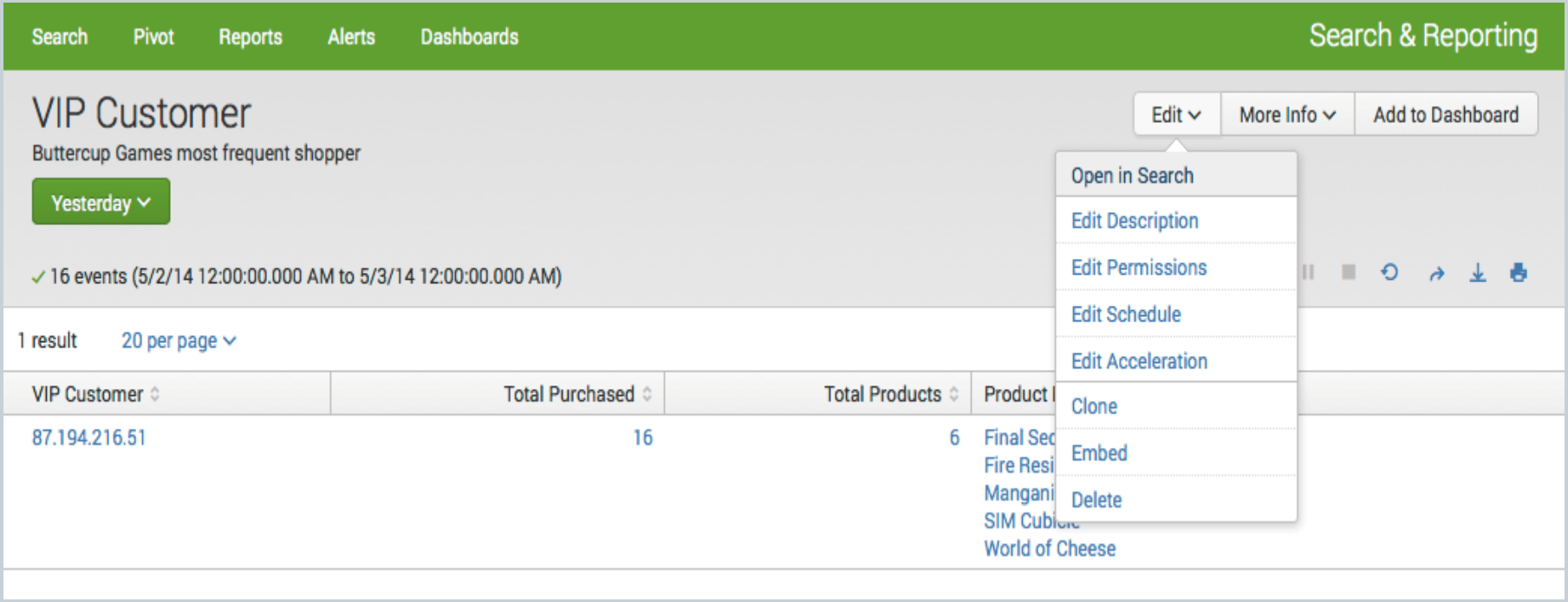
Saving and Sharing Reports

8. Click View.



Saving and Sharing Reports

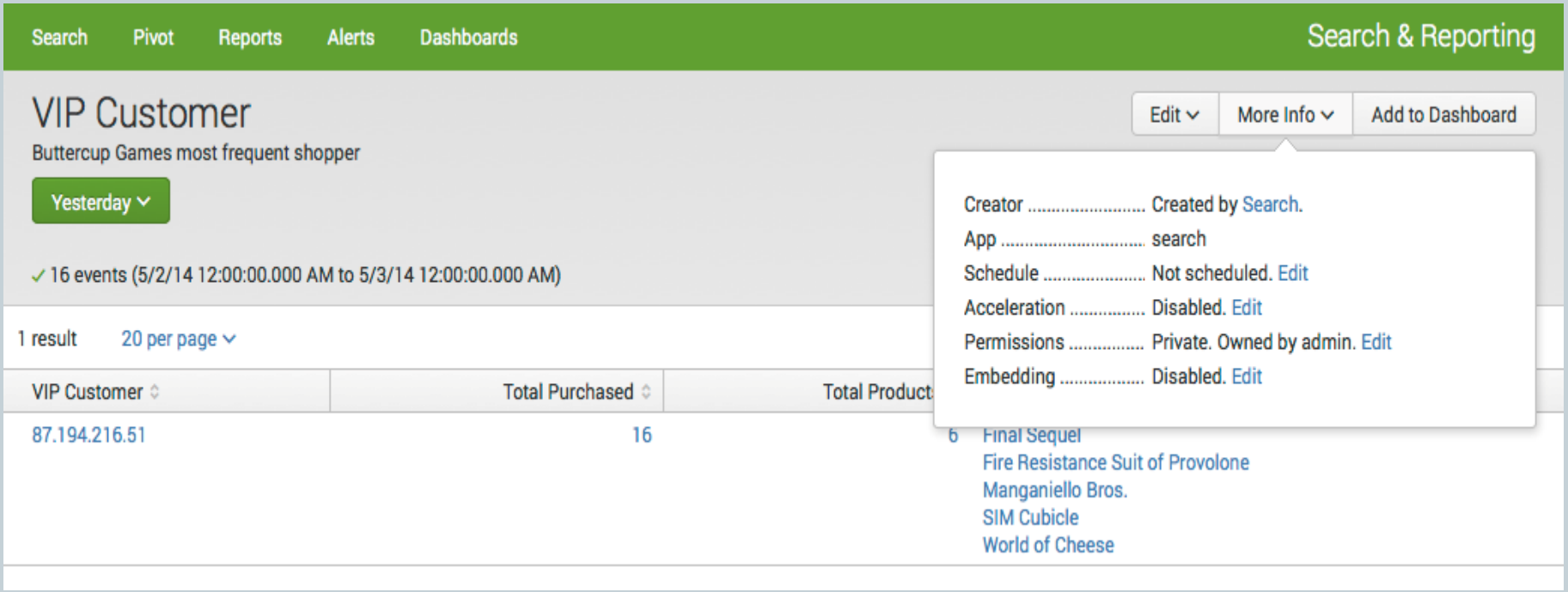
- **View and edit saved reports**
  You can view and edit the saved report from its report view.
  1. In the report view for "VIP Customer", click Edit.



You can open the report in the search view and edit the saved search's description, permissions, schedule, and acceleration. You can also clone, embed, and delete the report from this menu.

Saving and Sharing Reports

2. **Click More Info.**

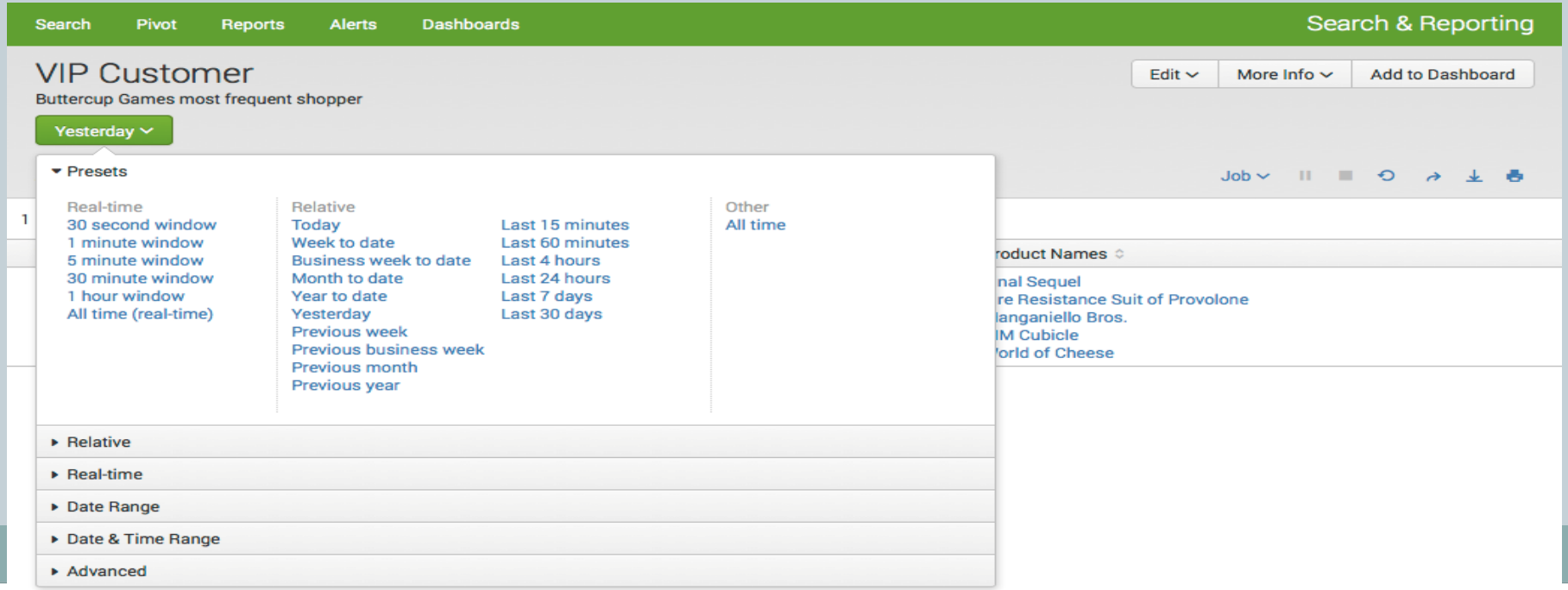


You can view and edit different properties of the report, including its schedule, acceleration, permissions, and embedding.

Saving and Sharing Reports

3. Look at the time range picker, located to the top left.

- You saved this report with a time range picker. The time range picker lets you change the time period to run this search. For example, you can use this time range picker to run this search for the VIP Customer Week to date, Last 60 minutes, Last 24 hours just by selecting the Preset time range or defining a custom time range.

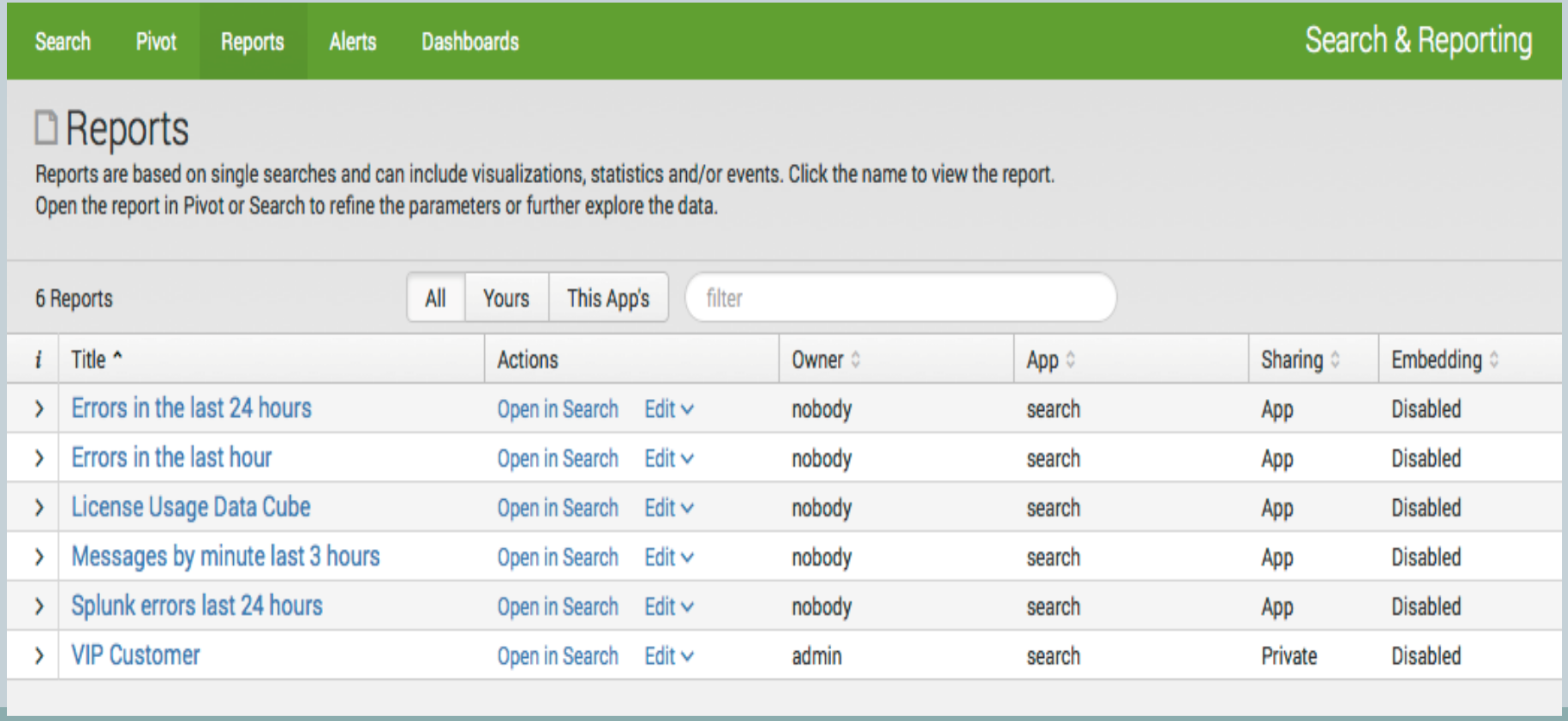


Saving and Sharing Reports

- Find and share saved reports

  You can access your saved reports using the app navigation bar.

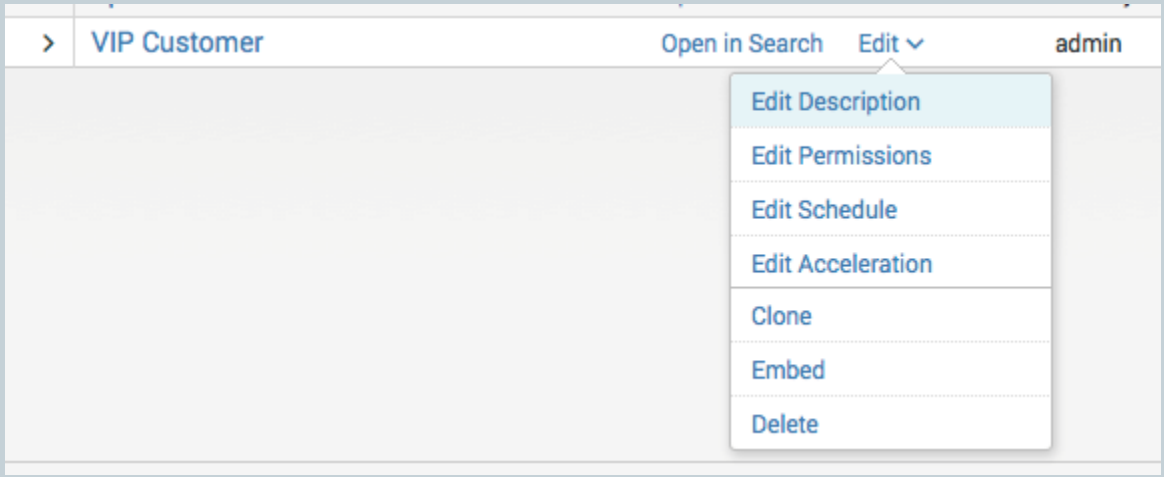
  1. Click Reports to open the Reports listing page.



Saving and Sharing Reports

When you save a new report, its Permissions are set to Private. This means that only you can view and edit the report. You can allow other apps to view, or edit, or view and edit the reports by changing its Permissions.

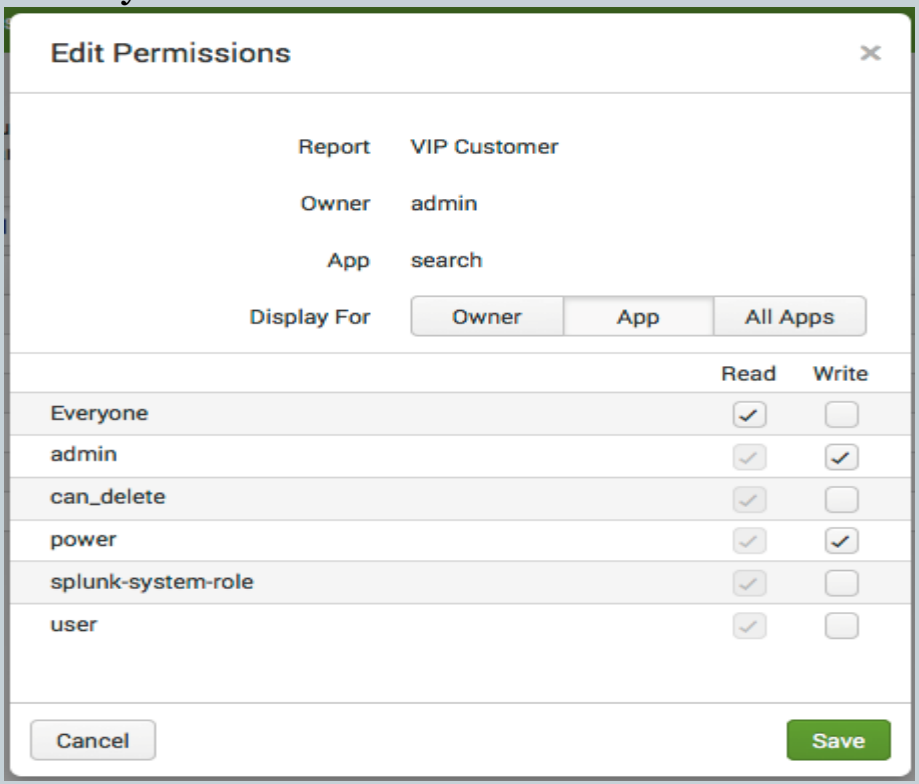
1. Under Actions for the VIP Customer report, click Edit and select Edit Permissions.



This opens the Edit Permissions dialog box.

Saving and Sharing Reports

2. In the Edit Permissions dialog box, set Display For to App and check the box under Read for Everyone.



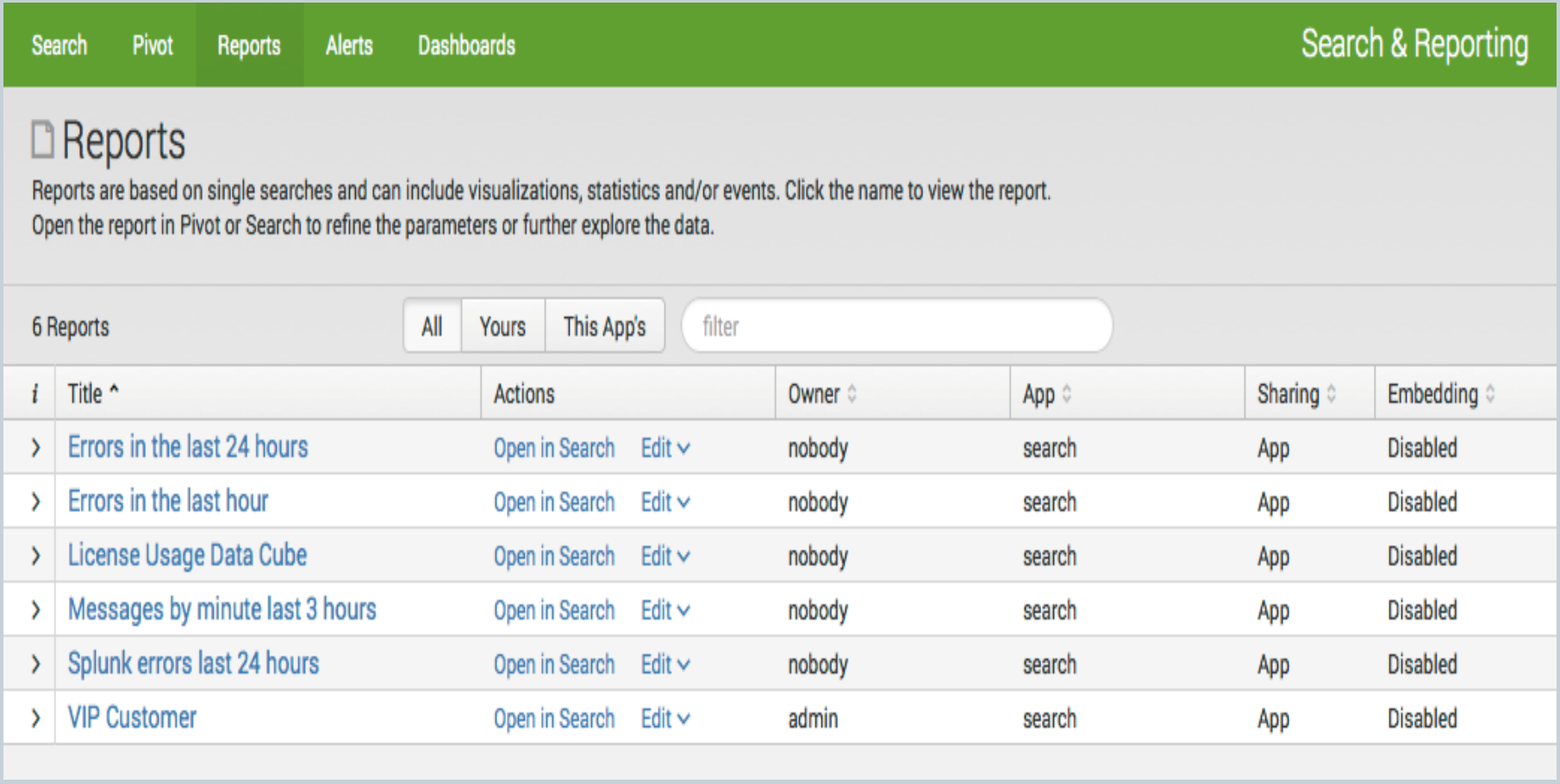
This action gives everyone who has access to this app the permission to view it.

3. Click Save.

KOENIG
step forward

Saving and Sharing Reports

Back at the Reports listing page, you see that the Sharing for VIP Customer now reads App.



More Searches and Reports

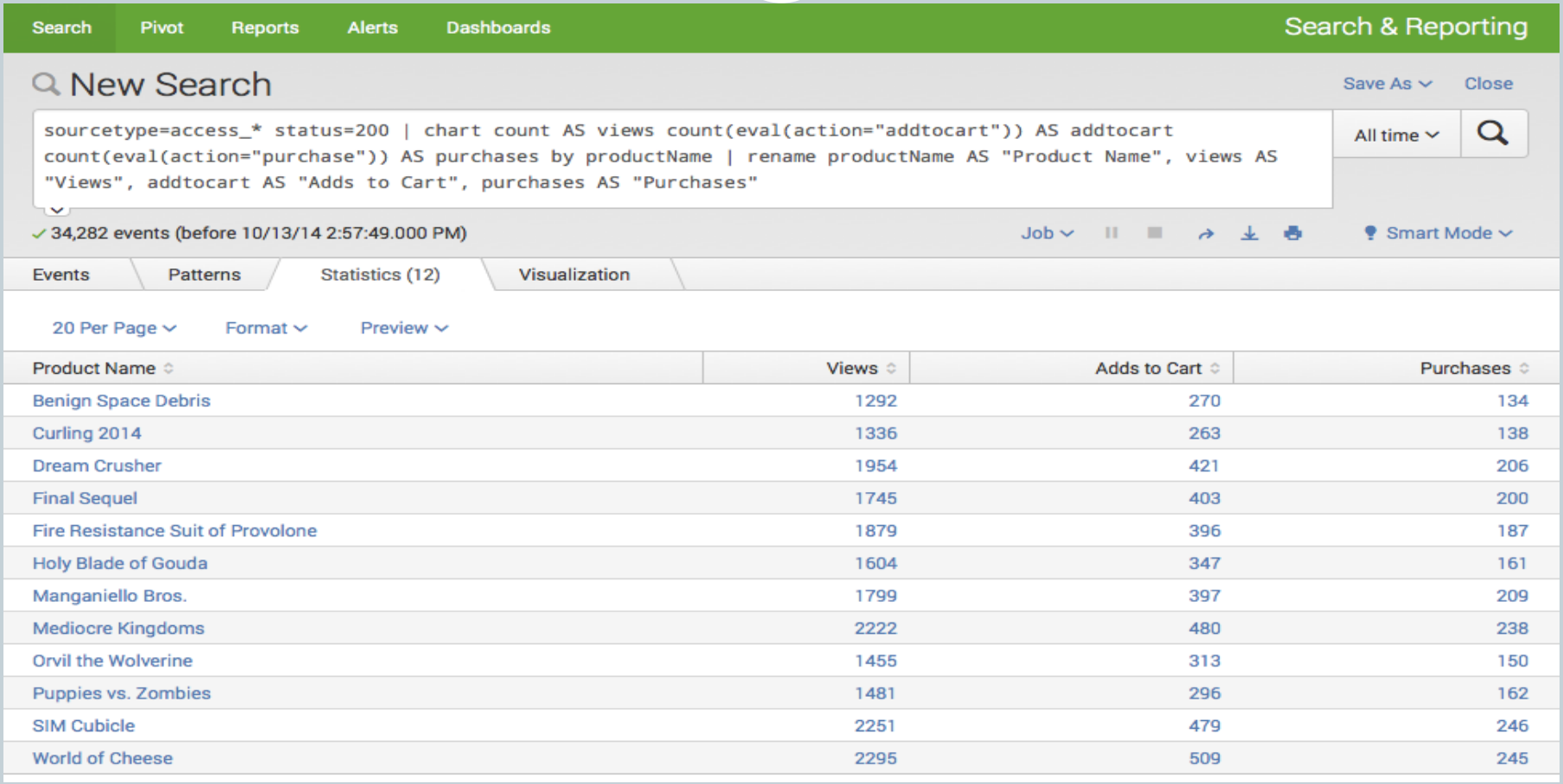
- **Example 1: Compare counts of user actions**

  In this example, calculate the number of views, purchases, and adds to cart for each type of product. This report requires the productName field from the fields lookup example. If you did not add the lookup, refer to that example and follow the procedure.

  1. Run this search:

  sourcetype=access_* status=200 | chart count AS views count(eval(action="addtocart")) AS addtocart count(eval(action="purchase")) AS purchases by productName | rename productName AS "Product Name", views AS "Views", addtocart AS "Adds to Cart", purchases AS "Purchases"

More Searches and Reports

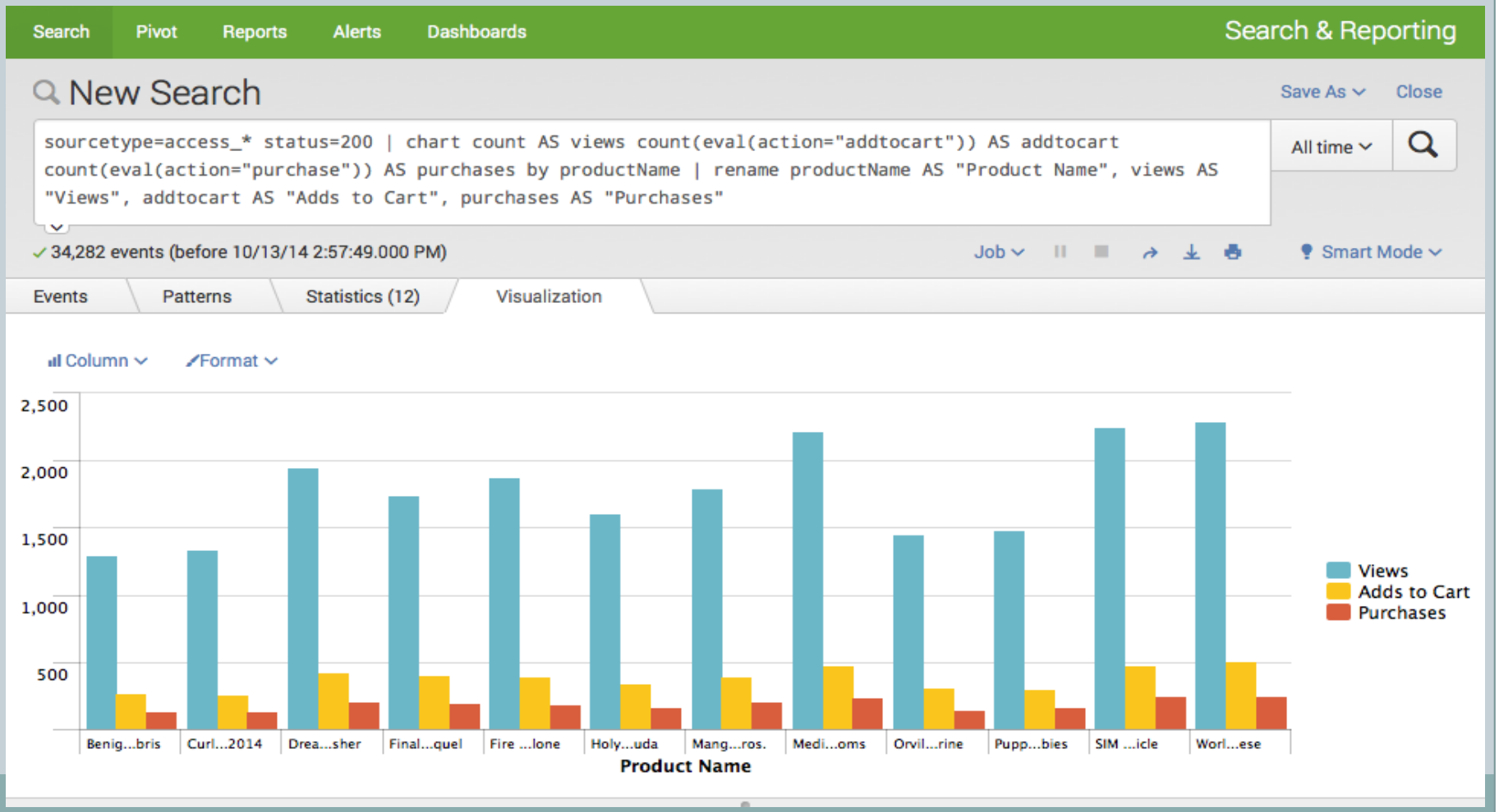


Product Name	Views	Adds to Cart	Purchases
Benign Space Debris	1292	270	134
Curling 2014	1336	263	138
Dream Crusher	1954	421	206
Final Sequel	1745	403	200
Fire Resistance Suit of Provolone	1879	396	187
Holy Blade of Gouda	1604	347	161
Manganiello Bros.	1799	397	209
Mediocre Kingdoms	2222	480	238
Orvil the Wolverine	1455	313	150
Puppies vs. Zombies	1481	296	162
SIM Cubicle	2251	479	246
World of Cheese	2295	509	245

This search uses the chart command to count the number of events that are action=purchase andaction=addtocart.

More Searches and Reports

2. Use the Visualization view options to format the results as a column chart.



KOENIG
step forward

More Searches and Reports

Example 2: Overlay Actions and Conversion Rates on one chart

1. Run this search:

```
sourcetype=access_* status=200 | stats count AS views count(eval(action="addtocart")) AS addtocart count(eval(action="purchase")) AS purchases by productName | eval viewsToPurchase=(purchases/views)*100 | eval cartToPurchase=(purchases/addtocart)*100 | table productName views addtocart purchases viewsToPurchase cartToPurchase | rename productName AS "Product Name" views AS "Views", addtocart as "Adds To Cart", purchases AS "Purchases“
```

Instead of the chart command, this search uses the stats command to count the user actions. Then, it uses the eval command to define two new fields which calculate conversation rates for "Product Views to Purchases" and "Adds to cart to Purchases".

KOENIG
step forward

More Searches and Reports

Search | Pivot | Reports | Alerts | Dashboards — Search & Reporting

New Search

Save As | Close

```
sourcetype=access_* status=200 | stats count AS views count(eval(action="addtocart")) AS addtocart
count(eval(action="purchase")) AS purchases by productName | eval viewsToPurchase=(purchases/views)*100 |
eval cartToPurchase=(purchases/addtocart)*100 | table productName views addtocart purchases viewsToPurchase
cartToPurchase | rename productName AS "Product Name" views AS "Views", addtocart as "Adds To Cart",
purchases AS "Purchases"
```

All time

✓ 34,282 events (before 10/13/14 4:13:37.000 PM)

Job | Smart Mode

Events | Patterns | Statistics (12) | Visualization

20 Per Page | Format | Preview

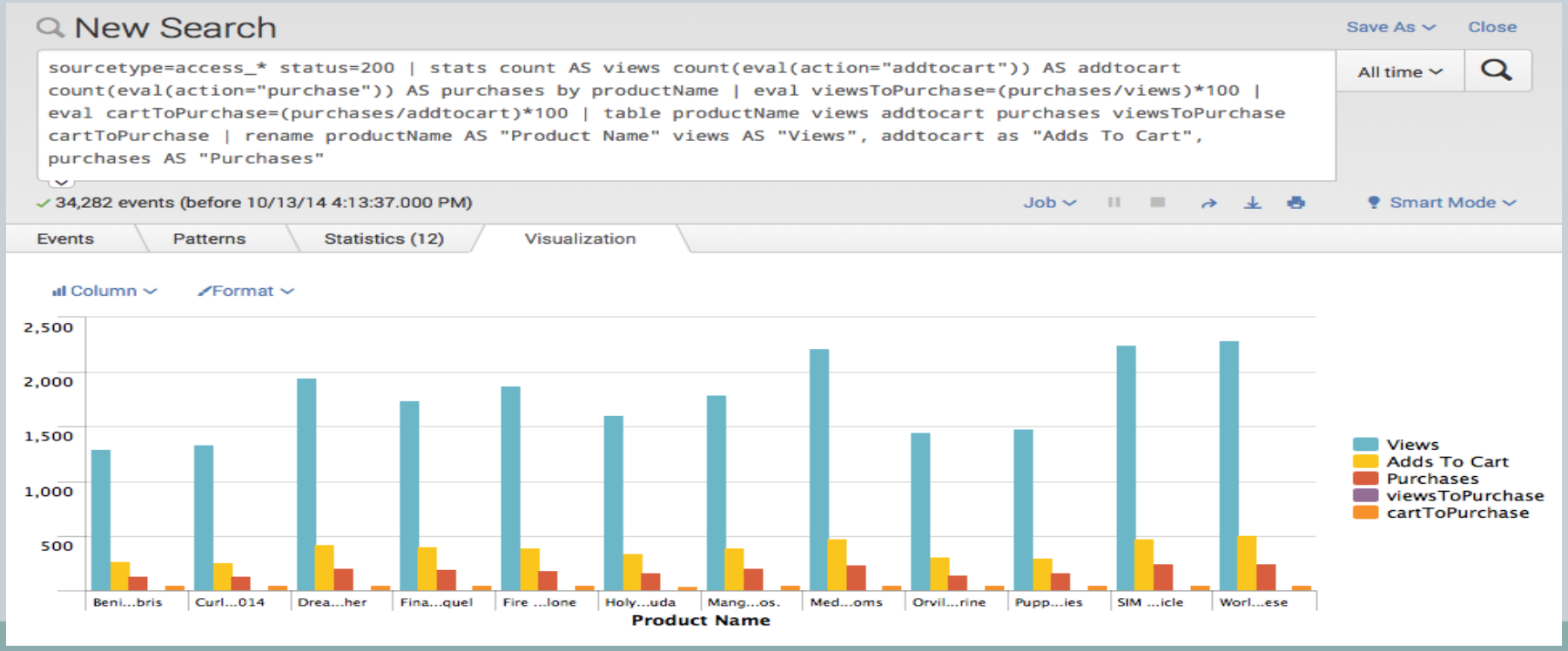
Product Name	Views	Adds To Cart	Purchases	viewsToPurchase	cartToPurchase
Benign Space Debris	1292	270	134	10.371517	49.629630
Curling 2014	1336	263	138	10.329341	52.471483
Dream Crusher	1954	421	206	10.542477	48.931116
Final Sequel	1745	403	200	11.461318	49.627792
Fire Resistance Suit of Provolone	1879	396	187	9.952102	47.222222
Holy Blade of Gouda	1604	347	161	10.037406	46.397695
Manganiello Bros.	1799	397	209	11.617565	52.644836
Mediocre Kingdoms	2222	480	238	10.711071	49.583333
Orvil the Wolverine	1455	313	150	10.309278	47.923323
Puppies vs. Zombies	1481	296	162	10.938555	54.729730
SIM Cubicle	2251	479	246	10.928476	51.356994
World of Cheese	2295	509	245	10.675381	48.133595

More Searches and Reports

- Steps 2 to 6 reformat the visualization to overlay the Conversion series onto the Actions series.

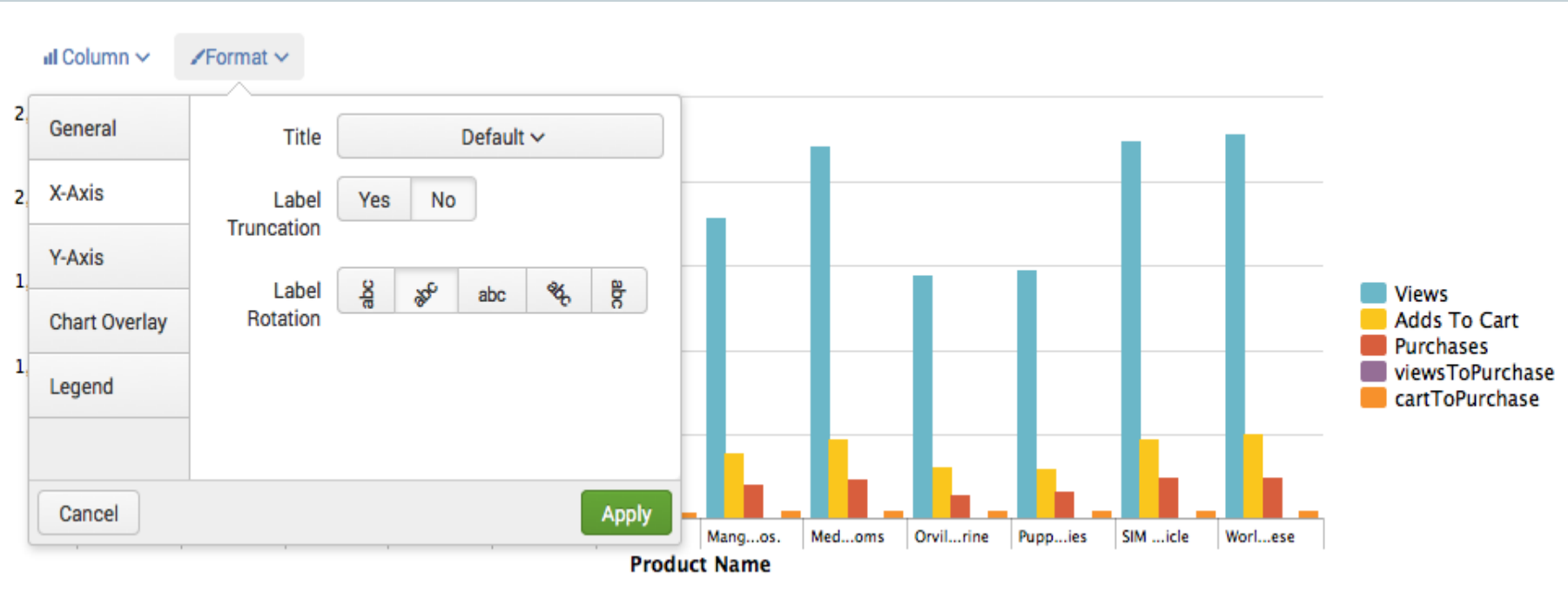
2. Click Visualization.

This is the same chart as in Example 1, with two additional series, "viewsToPurchase" and "cartToPurchase".



More Searches and Reports

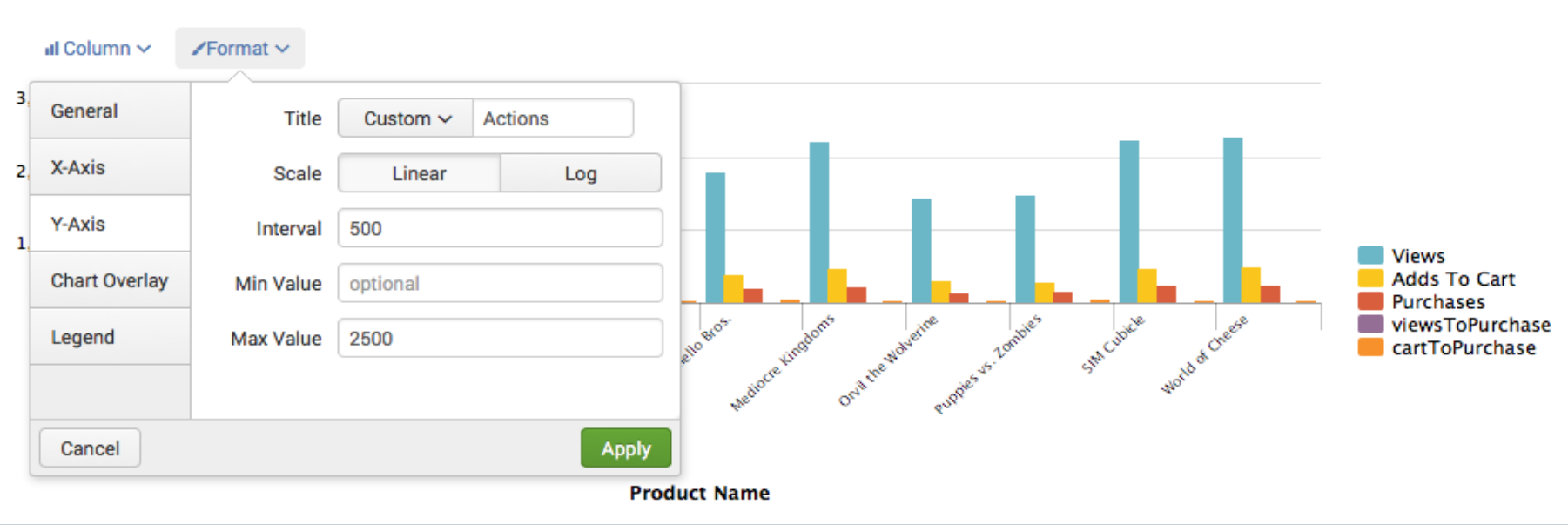
3. Click Format and X-Axis.



- 3.1 Rotate the label -45 degrees and do not truncate the label.
- 3.2 Click Apply.

More Searches and Reports

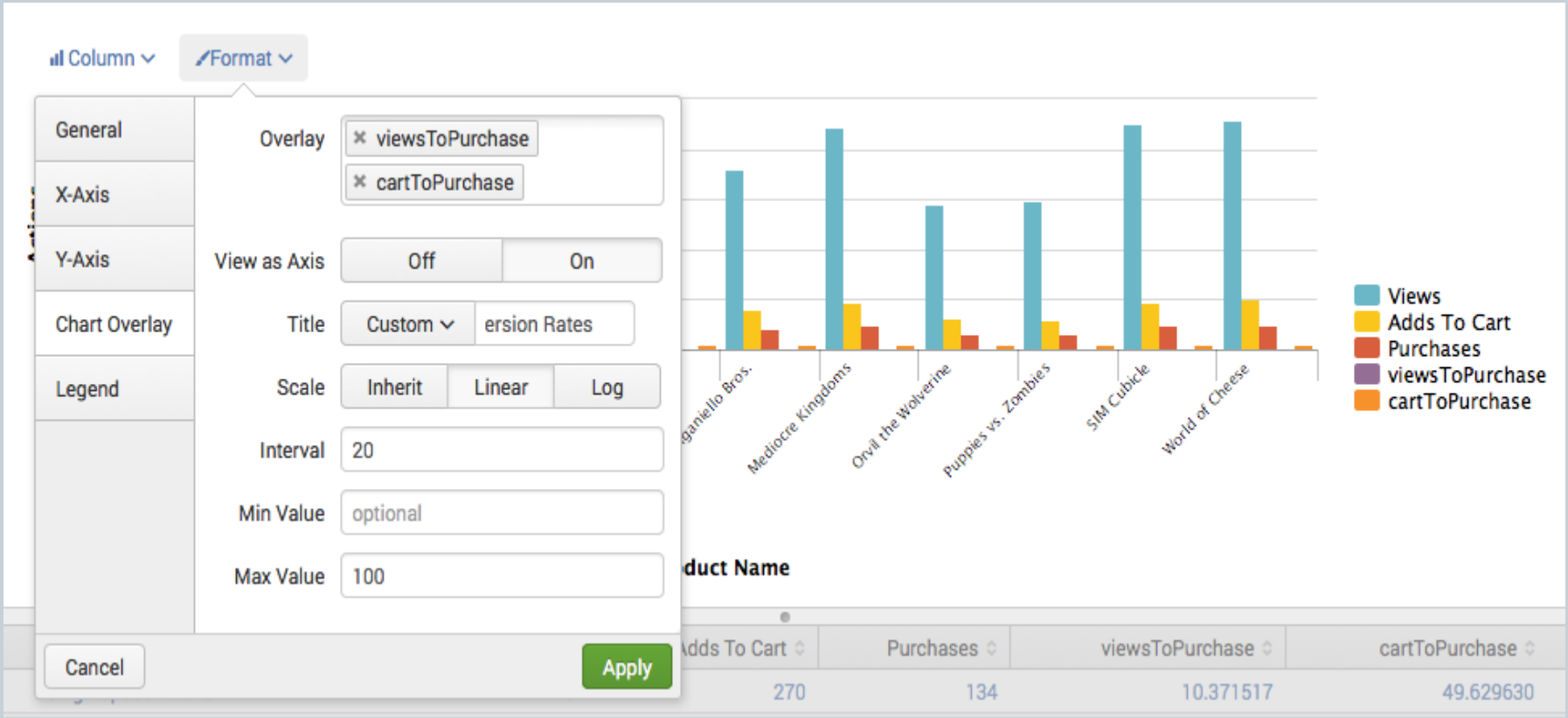
4. Click Format and Y-Axis.



- 4.1 For Title, choose Custom and type in "Actions".
- 4.2 Set the Max Value to 2500 and the Interval to 500.
- 4.3 Click Apply.

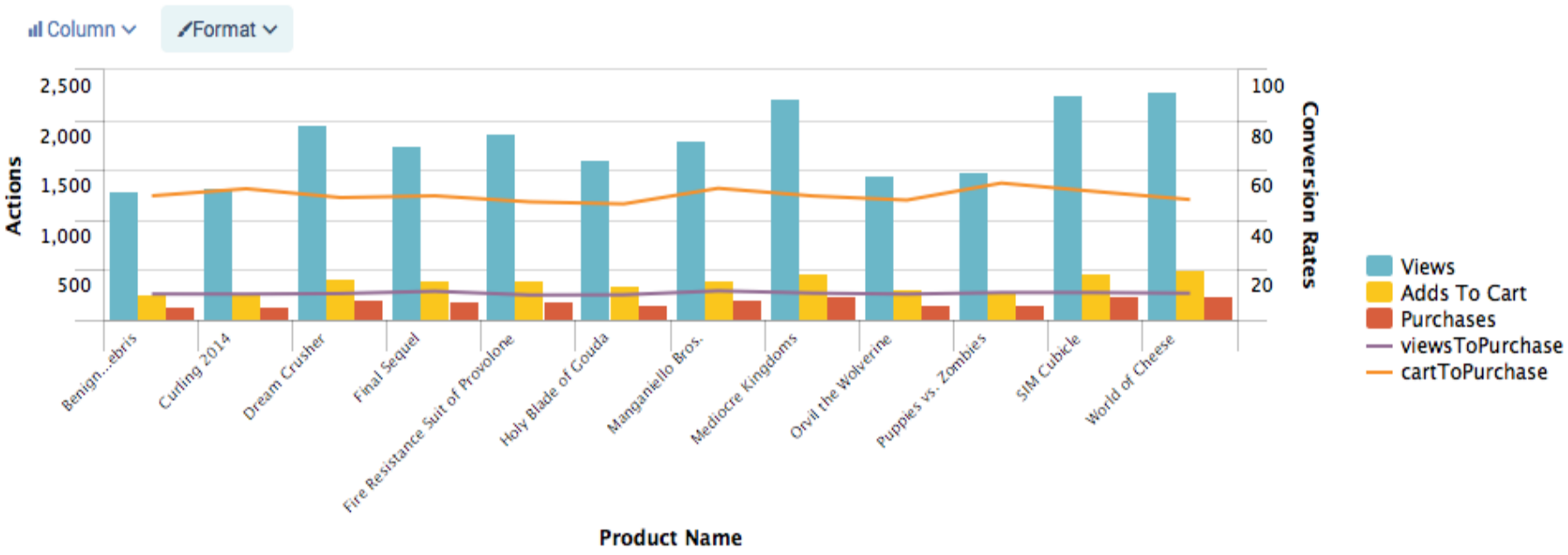
More Searches and Reports

5. Click Format and Chart Overlay.



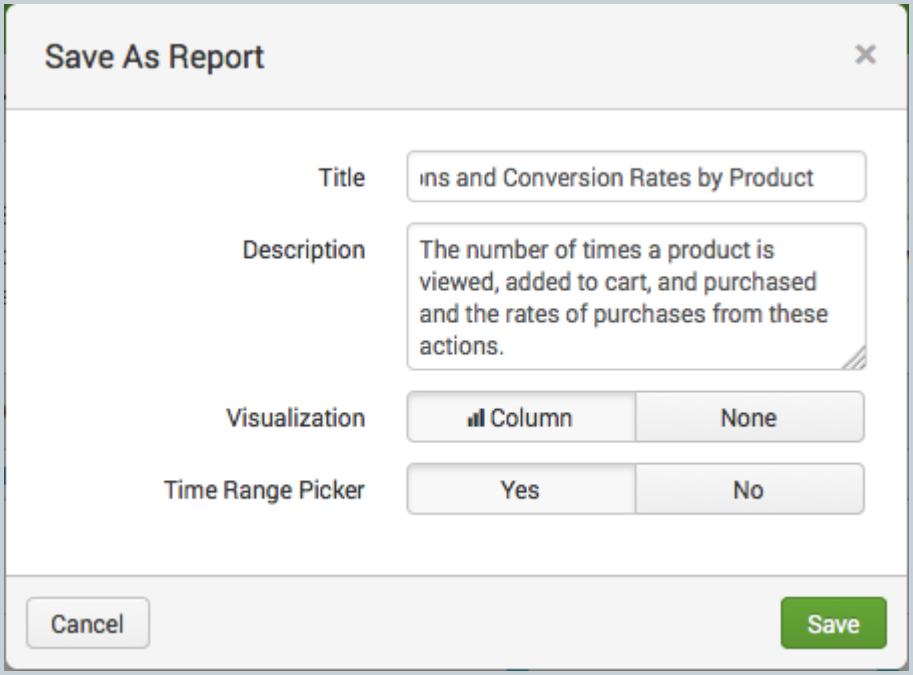
More Searches and Reports

- 5.1 Type in or select the fields, "viewsToPurchase" and "cartToPurchase".
- 5.2 For View as Axis, click On.
- 5.3 For Title, choose Custom and type in Conversion Rates.
- 5.4 For Scale, choose Linear.
- 5.5 Set the Max Value to 100 and the Interval to 20.
- 5.6 Click Apply.



More Searches and Reports

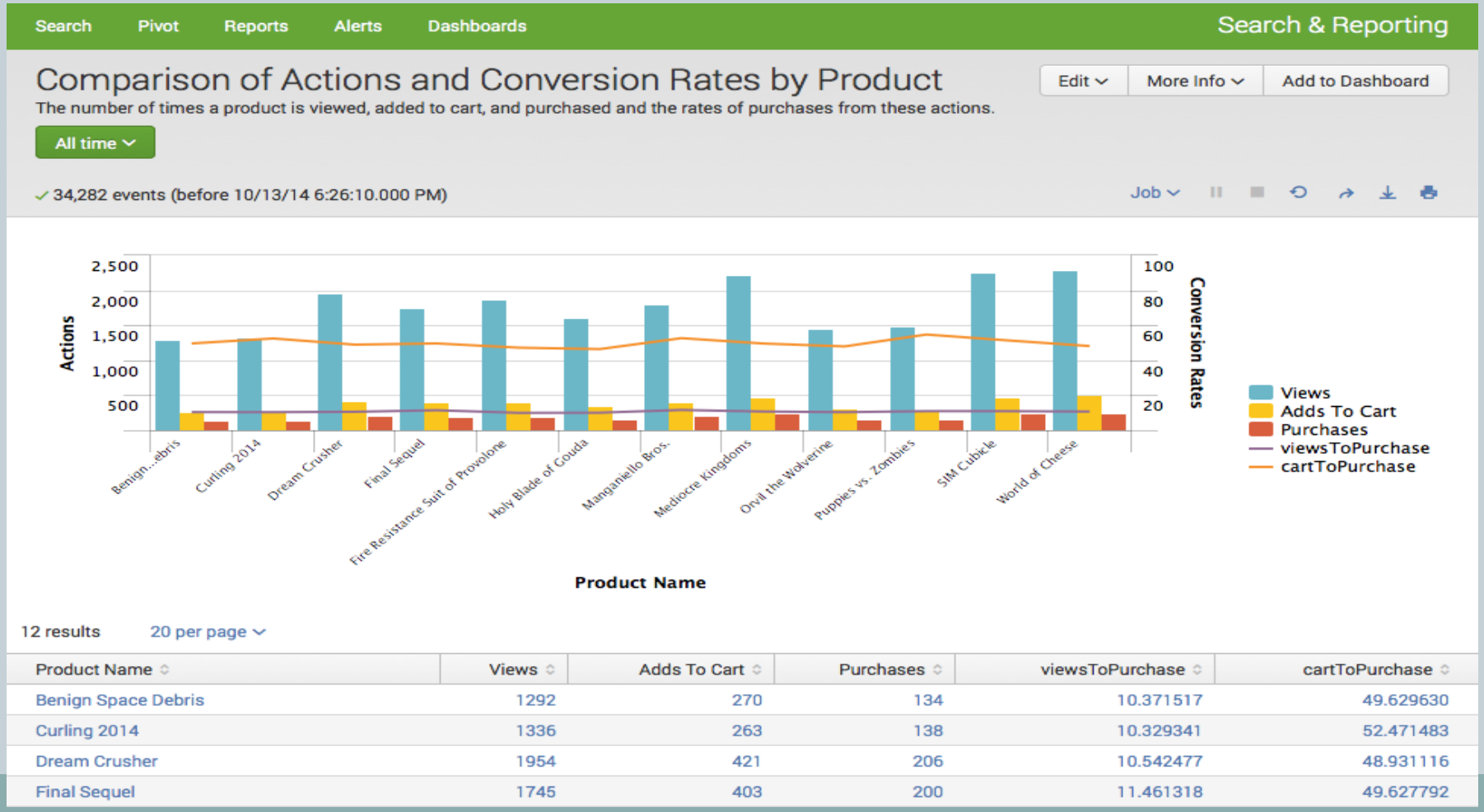
- 6. Click Save As and select Report.



- 6.1 In the Save Report As dialog box, enter a Title, "Comparison of Actions and Conversion Rates by Product".
- 6.2 (Optional) Enter a Description, "The number of times a product is viewed, added to cart, and purchased and the rates of purchases from these actions."

More Searches and Reports

- 7. Click Save.



Product Name	Views	Adds To Cart	Purchases	viewsToPurchase	cartToPurchase
Benign Space Debris	1292	270	134	10.371517	49.629630
Curling 2014	1336	263	138	10.329341	52.471483
Dream Crusher	1954	421	206	10.542477	48.931116
Final Sequel	1745	403	200	11.461318	49.627792

KOENIG
step forward

More Searches and Reports

Example 3: Products purchased over time

For this report, chart the number of purchases that were completed for each item.

This report requires the productName field from the fields lookup example. If you didn't add the lookup, refer to that example and follow the procedure.

1. Search for:

   sourcetype=access_* | timechart count(eval(action="purchase")) by productName usenull="f" useother="f"

   Use the count() function to count the number of events that have the field action=purchase. Use the usenulland useother arguments to make sure the chart counts events that have a value for productName.

   This produces the following statistics table.

KOENIG
step forward

More Searches and Reports

Search | Pivot | Reports | Alerts | Dashboards — Search & Reporting

New Search

Save As | Close

```
sourcetype=access_* | timechart count(eval(action="purchase")) by productName usenull="f" useother="f"
```

All time

✓ 39,532 events (before 10/13/14 5:51:03.000 PM)

Job | Smart Mode

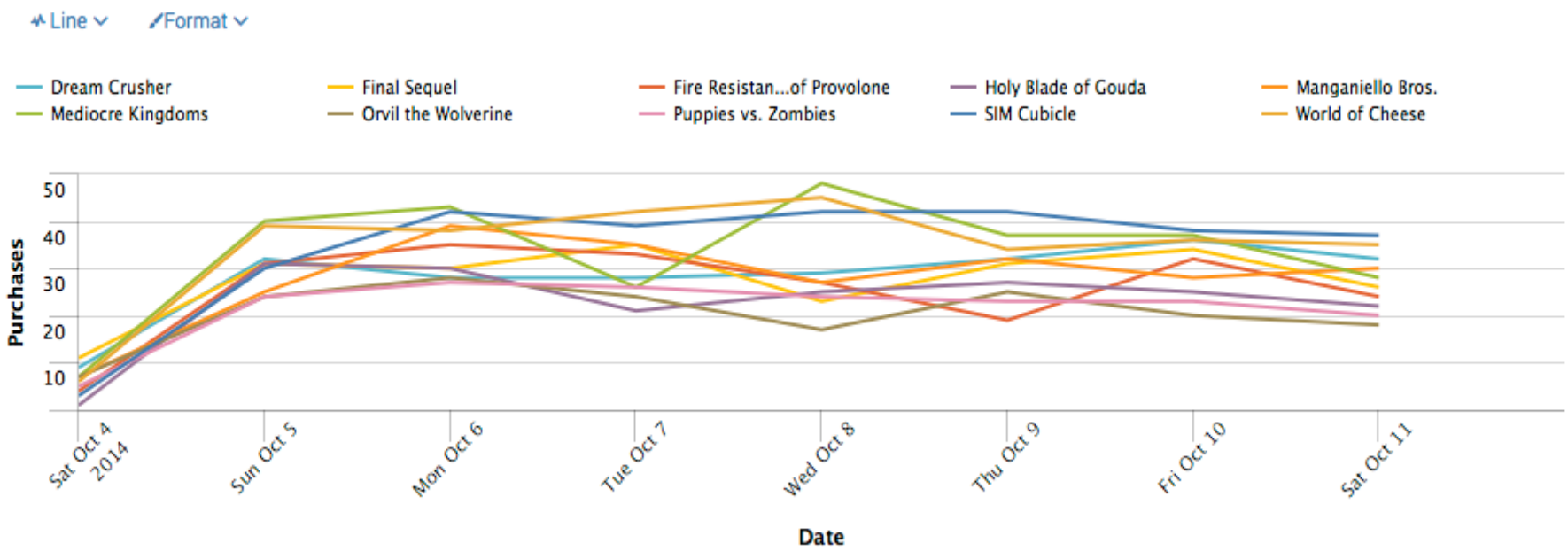
Events | Patterns | Statistics (8) | Visualization

20 Per Page | Format | Preview

_time	Dream Crusher	Final Sequel	Fire Resistance Suit of Provolone	Holy Blade of Gouda	Manganiello Bros.	Mediocre Kingdoms	Orvil the Wolverine	Puppies vs. Zombies	SIM Cubicle	World of Cheese
2014-10-04	9	11	4	1	7	7	7	5	3	6
2014-10-05	32	31	31	31	25	40	24	24	30	39
2014-10-06	28	30	35	30	39	43	28	27	42	38
2014-10-07	28	35	33	21	35	26	24	26	39	42
2014-10-08	29	23	27	25	27	48	17	24	42	45
2014-10-09	32	31	19	27	32	37	25	23	42	34
2014-10-10	36	34	32	25	28	37	20	23	38	36
2014-10-11	32	26	24	22	30	28	18	20	37	35

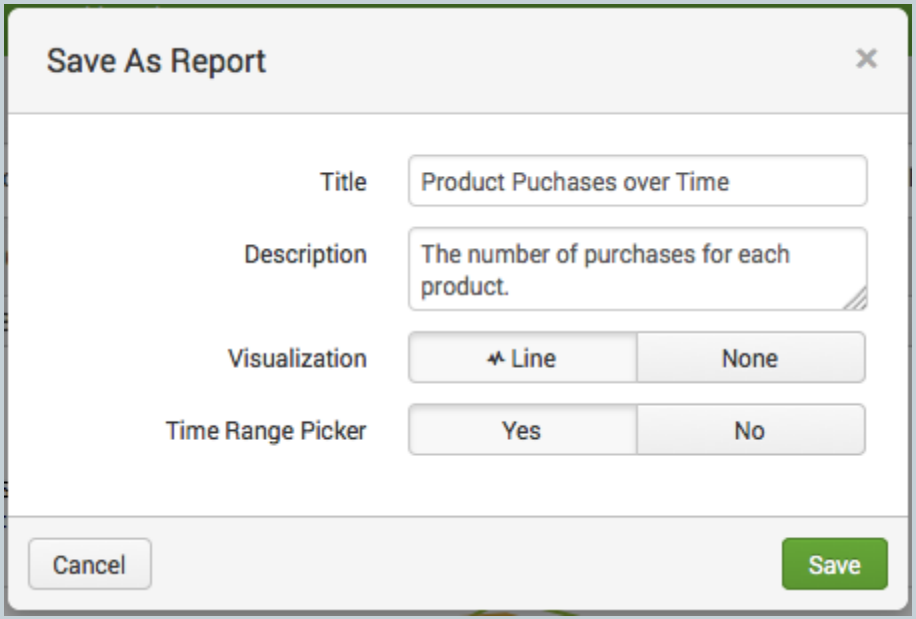
More Searches and Reports

2. Click the Visualization tab and Format the X-Axis, Y-Axis, and Legend to produce the following line chart.



More Searches and Reports

3. Click Save As and select Report



- 3.1 In the Save Report As dialog box, enter a Title, "Product Purchases over Time".
- 3.2 (Optional) Enter a Description, "The number of purchases for each product."

More Searches and Reports

4. Click Save and View the report.

Search Pivot Reports Alerts Dashboards Search & Reporting

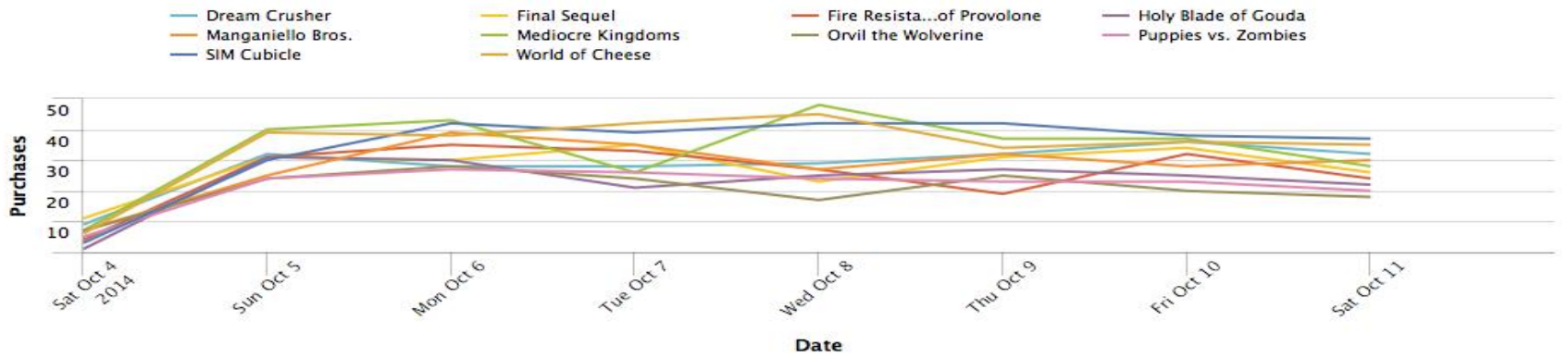
Product Puchases over Time

The number of purchases for each product.

Edit More Info Add to Dashboard

All time

✓ 39,532 events (before 10/13/14 6:28:29.000 PM) Job



8 results 20 per page

_time	Dream Crusher	Final Sequel	Fire Resistance Suit of Provolone	Holy Blade of Gouda	Manganiello Bros.	Mediocre Kingdoms	Orvil the Wolverine	Puppies vs. Zombies	SIM Cubicle	World of Cheese
2014-10-04	9	11	4	1	7	7	7	5	3	6
2014-10-05	32	31	31	31	25	40	24	24	30	39

KOENIG
step forward

More Searches and Reports

Example 4: Purchasing trends

This example uses sparklines to trend the count of purchases made over time.

For stats and chart searches, you can add sparklines to their results tables. Sparklines are inline charts that appear within the search results table and are designed to display time-based trends associated with the primary key of each row.

This example requires the productName field from the fields lookup example. If you did not add the lookup, refer to that example and follow the procedure.

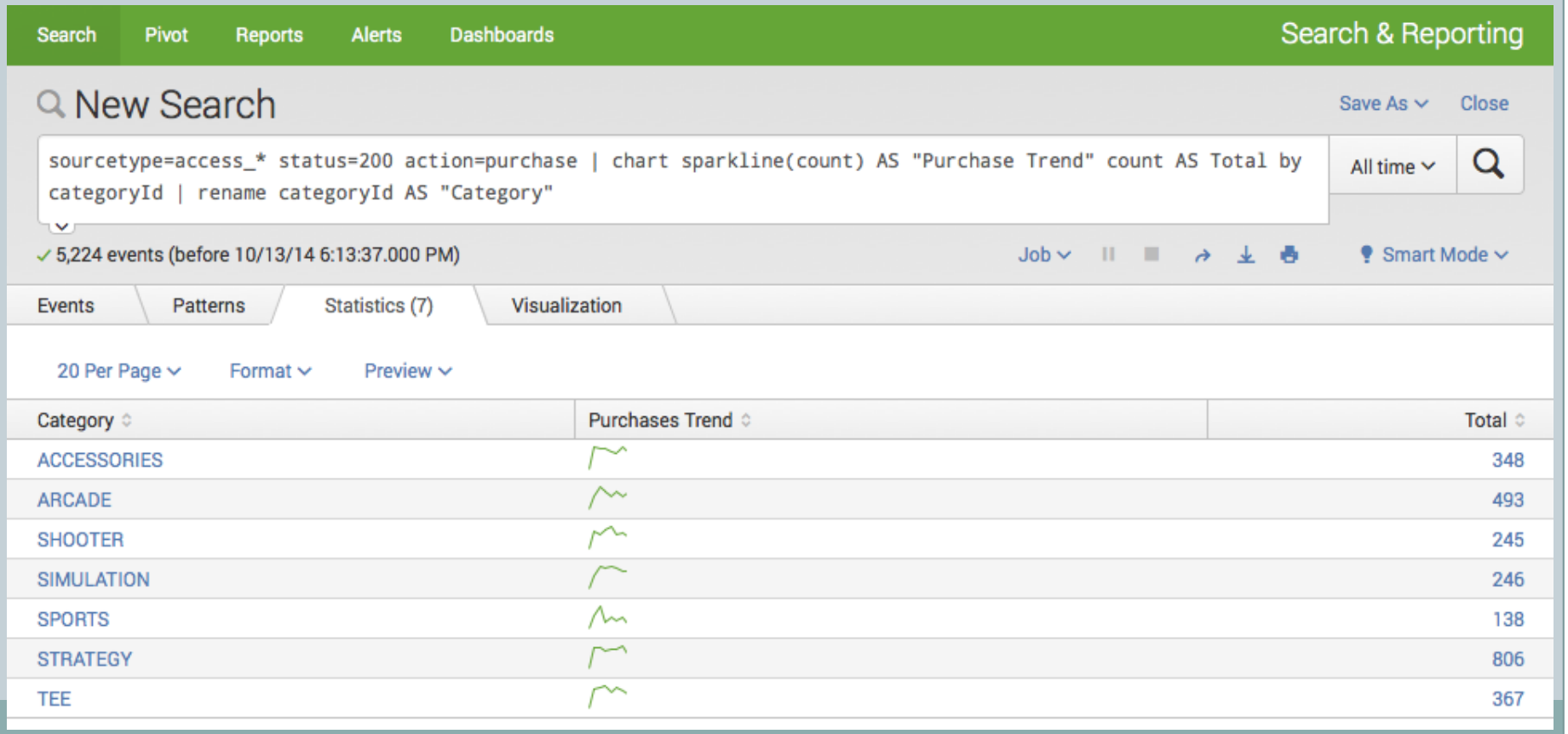
1. Run the following search:

sourcetype=access_* status=200 action=purchase| chart sparkline(count) AS "Purchases Trend" count AS Total by categoryId | rename categoryId AS "Category"

KOENIG
step forward

More Searches and Reports

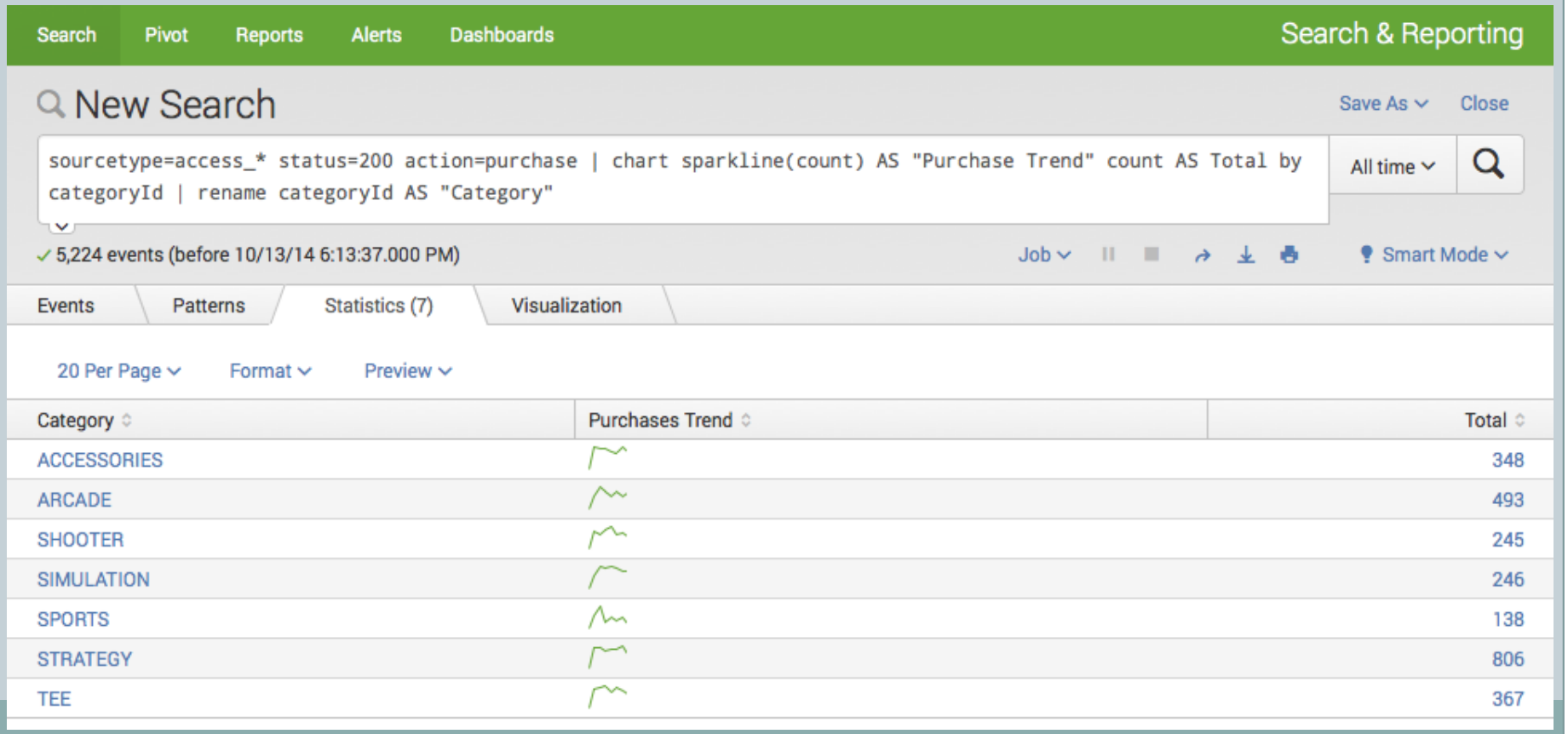
This search uses the chart command to count the number of purchases, action="purchase", made for each product, productName. The difference is that the count of purchases is now an argument of the sparkline()function.



KOENIG
step forward

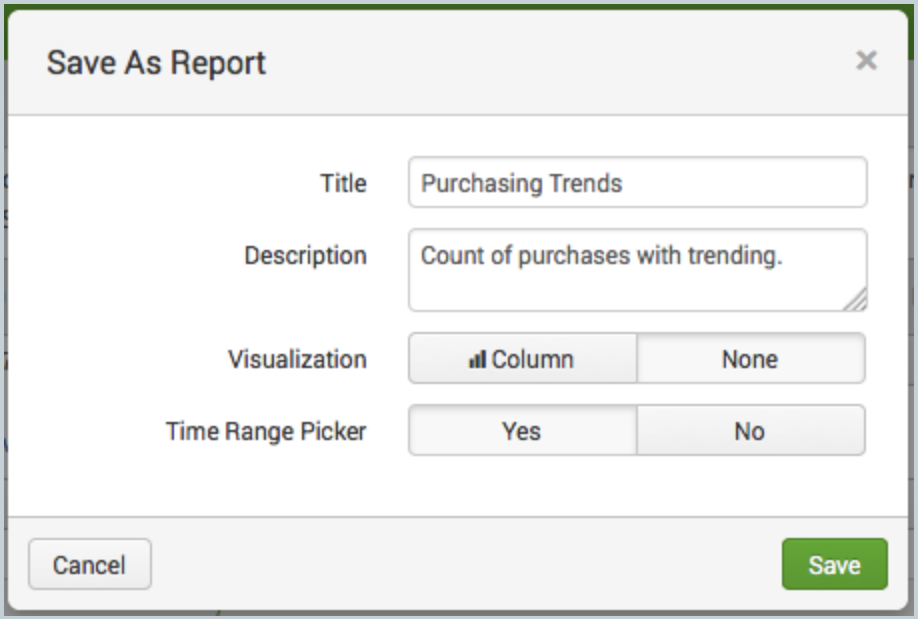
More Searches and Reports

This search uses the chart command to count the number of purchases, action="purchase", made for each product, productName. The difference is that the count of purchases is now an argument of the sparkline()function.



More Searches and Reports

3. Click Save As and select Report.



4. In the Save Report As dialog box, enter a Title, "Purchasing trends".
5. (Optional) Enter a Description, "Count of purchases with trending."
6. Click Save and View the report.

KOENIG
step forward

DASHBOARDS

- Dashboards are views that are made up of panels that can contain modules such as search boxes, fields, charts, tables, and lists. Dashboard panels are usually hooked up to saved searches.

- After you create a visualization or report, you can add it to a new or existing dashboard using the Save as report dialog box. You can also use the Dashboard Editor to create dashboards and edit existing dashboards. Using the Dashboard editor is useful when you have a set of saved reports that you want to quickly add to a dashboard.

KOENIG
step forward

DASHBOARDS

- **Change dashboard permissions**
- You can specify access to a dashboard from the Dashboard Editor. However, your user role (and capabilities defined for that role) might limit the type of access you can define.
- If your Splunk user role is admin (with the default set of capabilities), then you can create dashboards that are private, visible in a specific app, or visible in all apps. You can also provide access to other Splunk user roles, such as user, admin, and other roles with specific capabilities.

- **Change dashboard panel visualizations**
- After you create a panel with the Dashboard Editor, use the Visualization Editor to change the visualization type in the panel, and to determine how that visualization displays and behaves. The Visualization Editor lets you choose from visualization types that have their data structure requirements matched by the search that has been specified for the panel.

KOENIG
step forward

DASHBOARDS

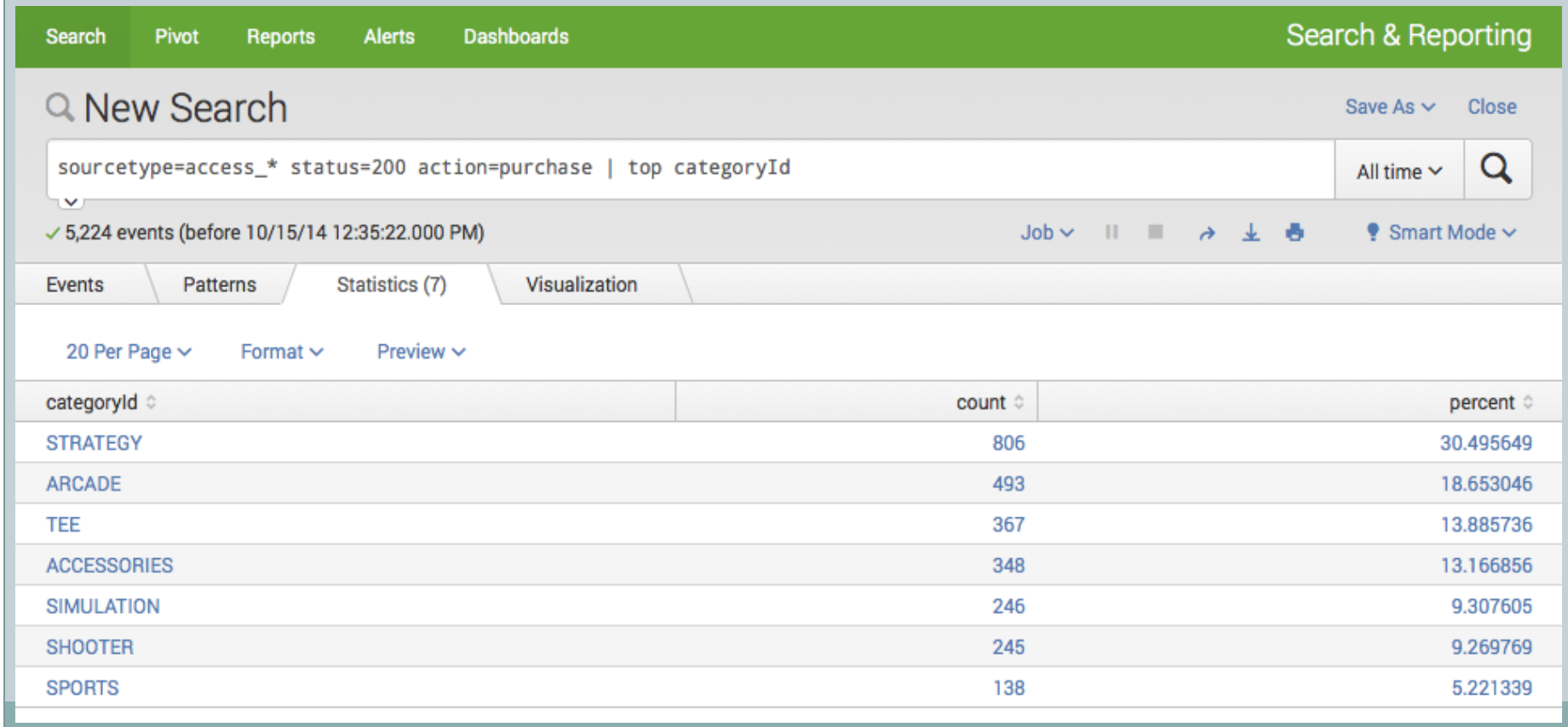
Creating dashboards and dashboard panels

DASHBOARDS

- **Save a search as a dashboard panel**

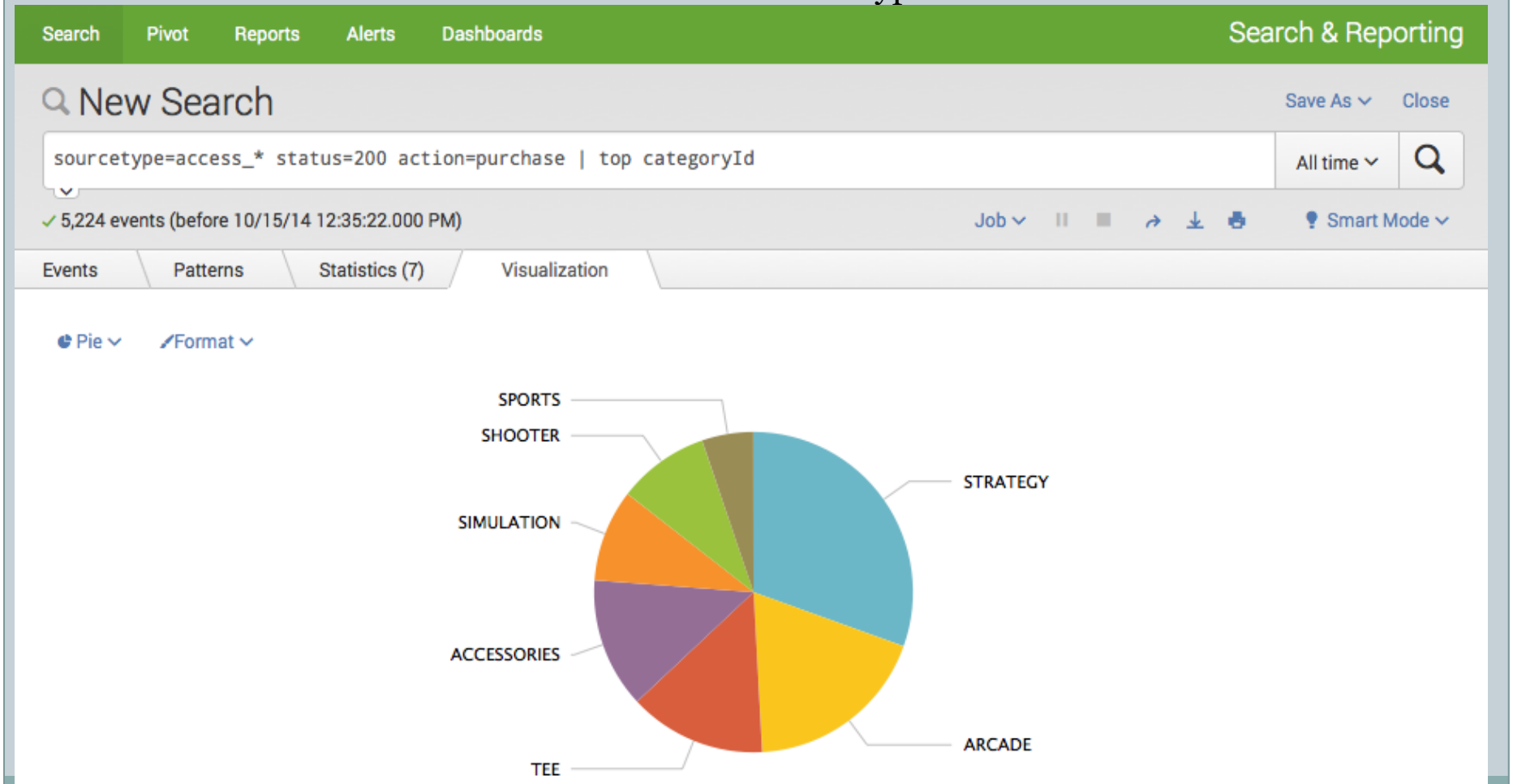
  1. Run the following search:

  sourcetype=access_* status=200 action=purchase | top categoryId



DASHBOARDS

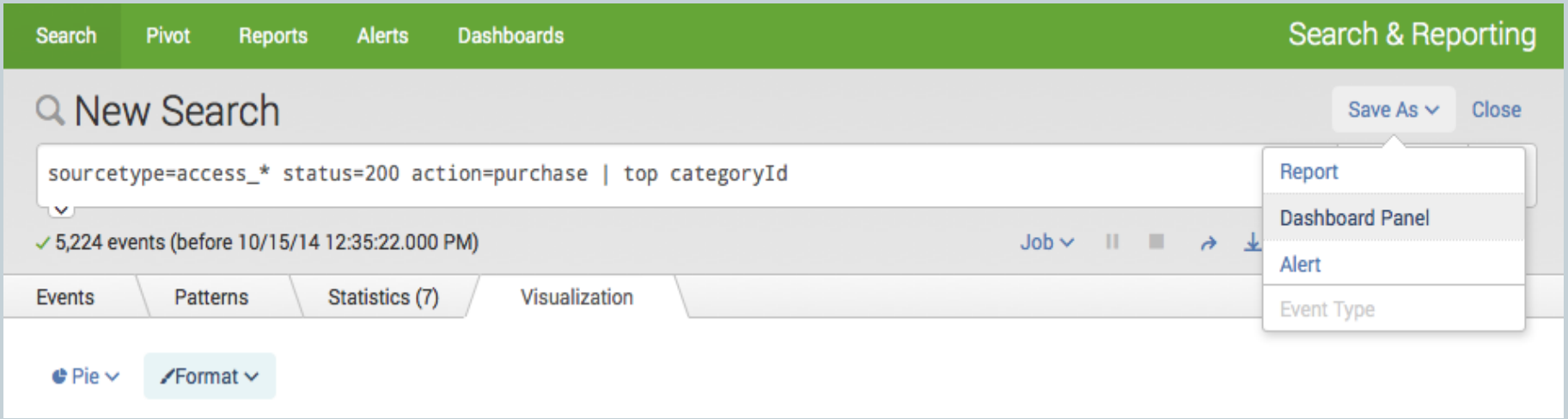
2. Click the Visualization tab and select the Pie chart type.



KOENIG
step forward

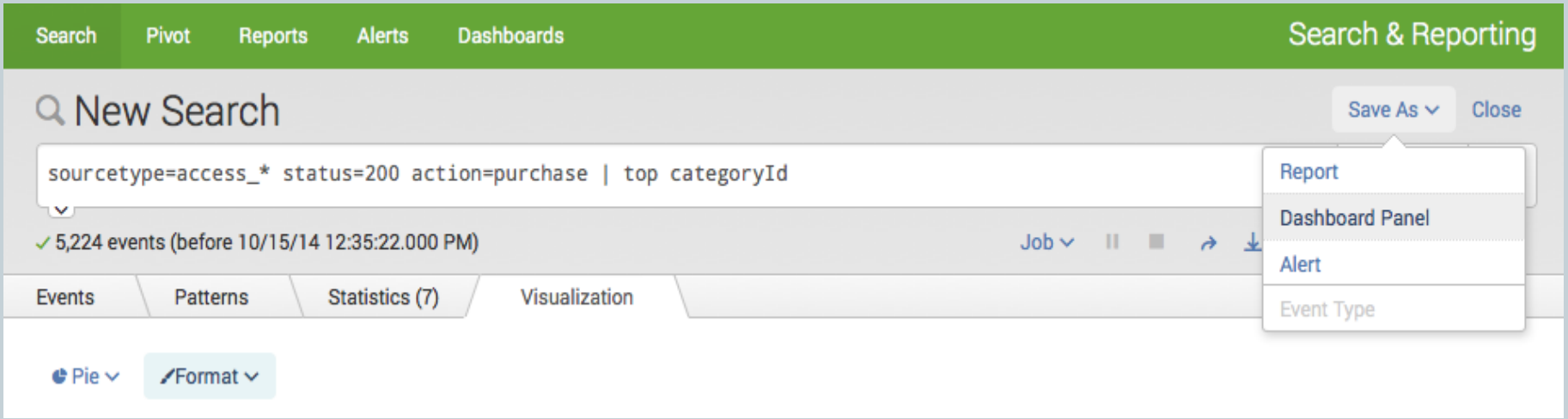
DASHBOARDS

3. In the Search view, click Save as and select Dashboard Panel.



DASHBOARDS

3. In the Search view, click Save as and select Dashboard Panel.

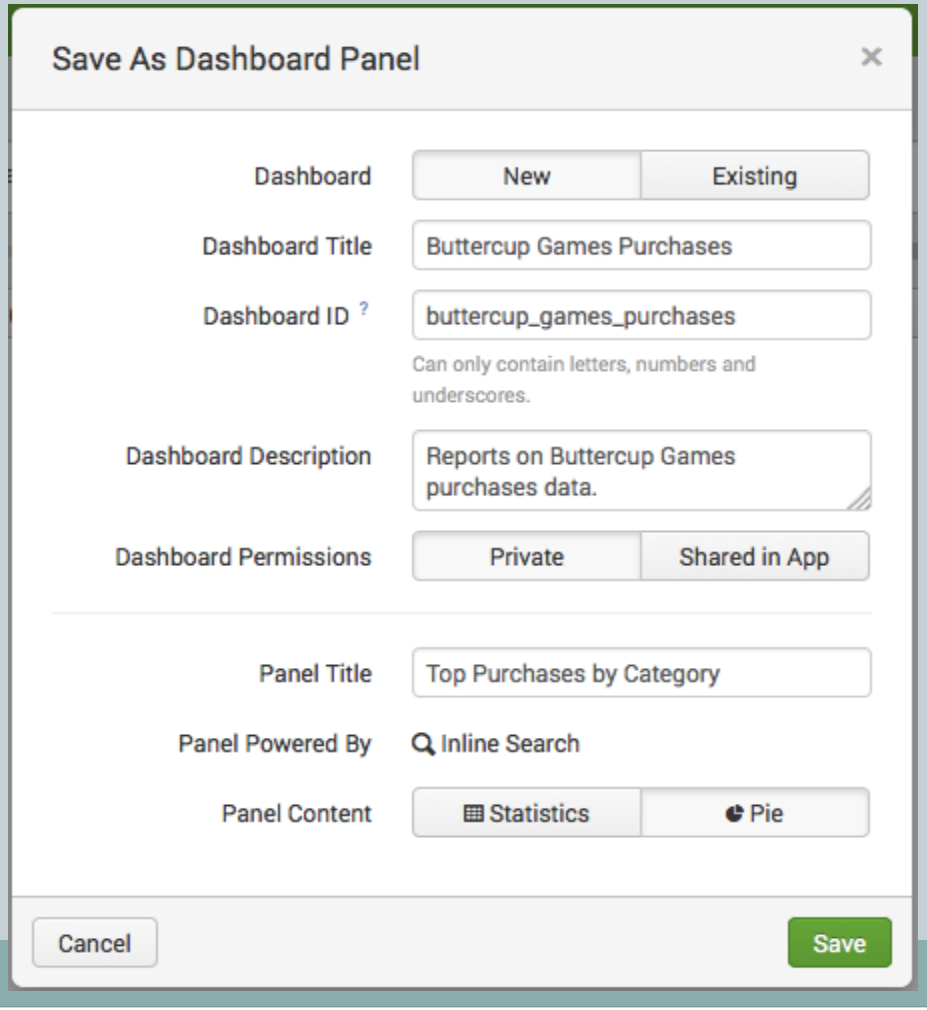


The Save as Dashboard Panel dialog box opens.

KOENIG
step forward

DASHBOARDS

4. Define a new dashboard and dashboard panel.



KOENIG
step forward

DASHBOARDS

4.1. For Dashboard, click New.

4.2. Enter the Dashboard Title, "Buttercup Games Purchases", The Dashboard ID updates with "Buttercup_games_purchases".

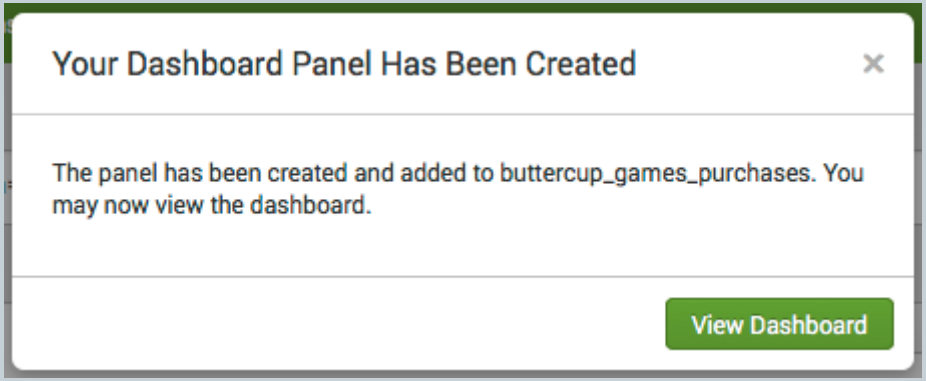
4.3. (Optional) Add a Dashboard Description, "Reports on Buttercup Games purchases data".

4.4. Type in the Panel Title, "Top Purchases by Category"

4.5. Leave the Panel Powered By as Inline search.

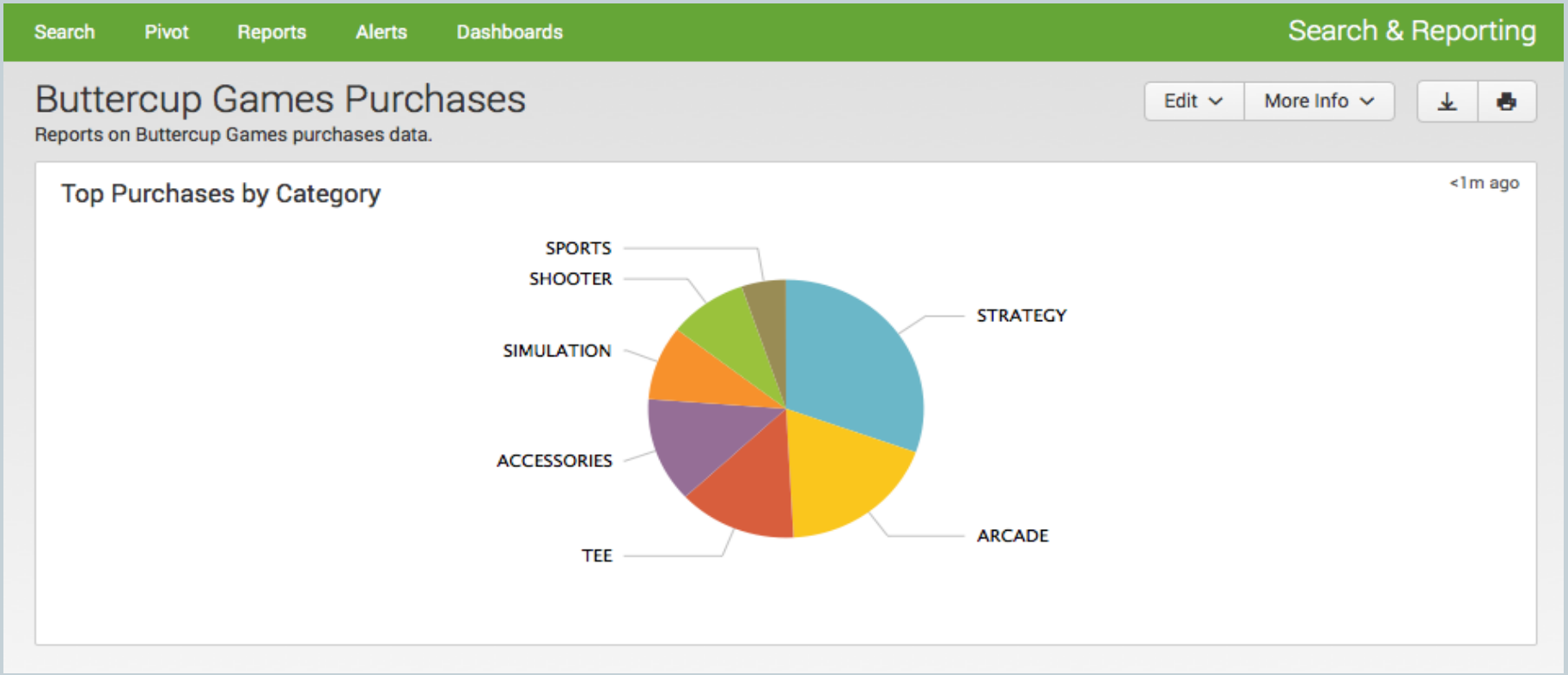
DASHBOARDS

5. Click Save.



DASHBOARDS

6. Click View Dashboard.



This creates a dashboard with one report panel. To add more report panels, you can run new searches and save them to this dashboard, or you can add saved reports.

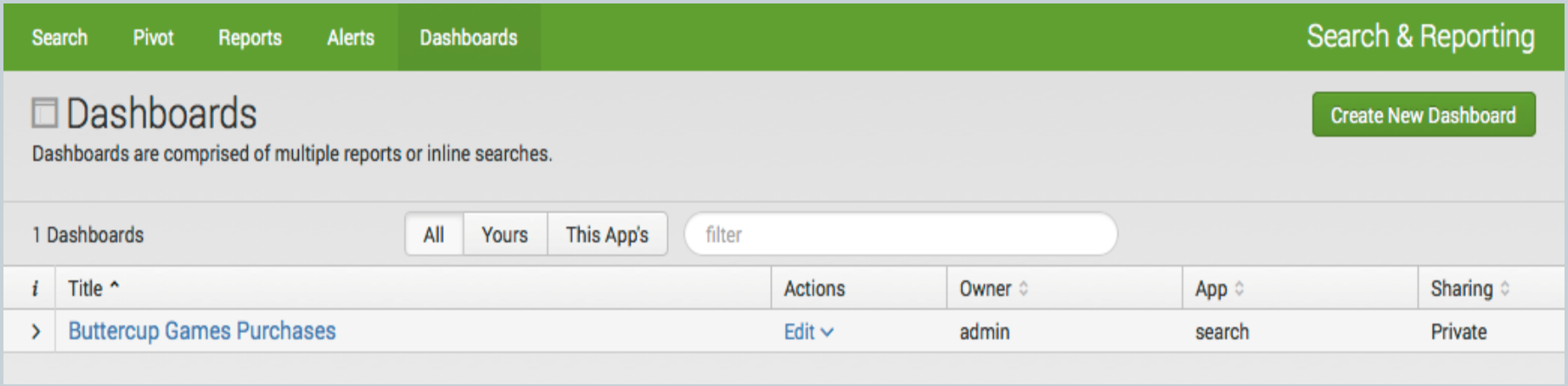
KOENIG
step forward

DASHBOARDS

- View and edit dashboard panels

DASHBOARDS

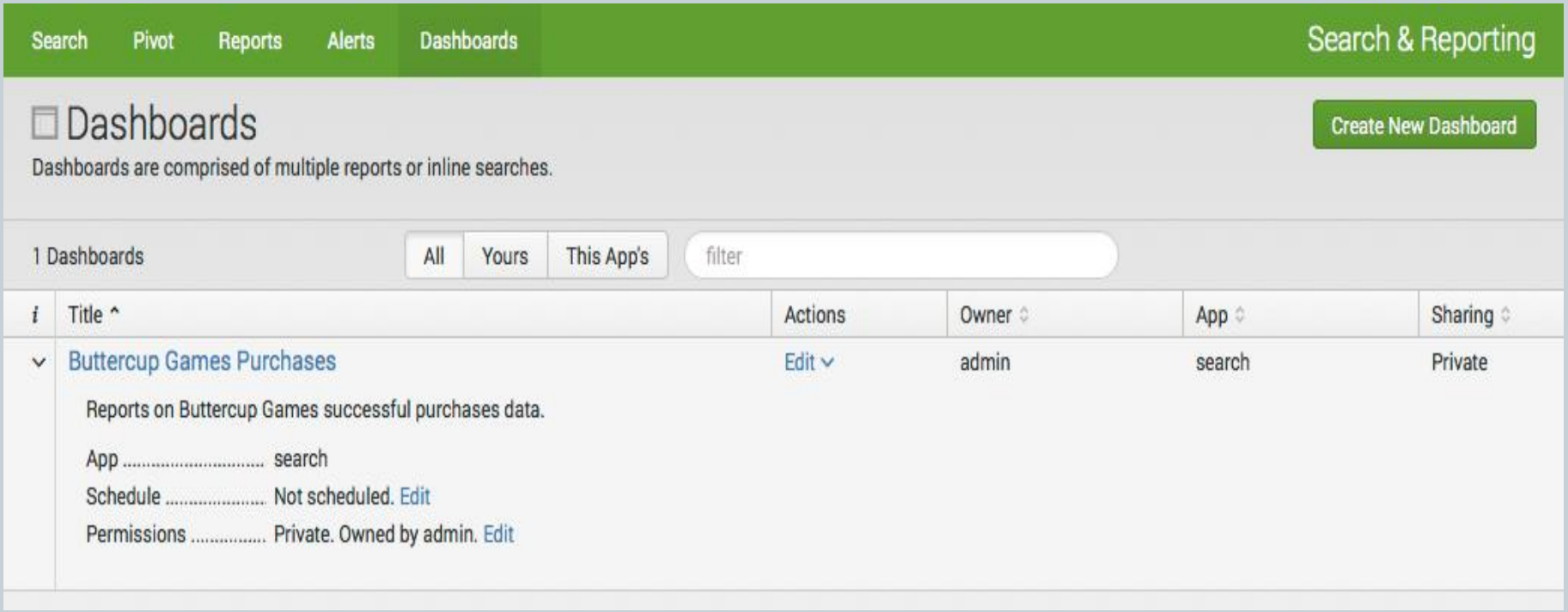
1. Click Dashboards in the app navigation bar.
   This takes you to the Dashboards listing page.



You can Create a new dashboard and edit existing dashboards. You see the Buttercup Games Purchasesdashboard that you created.

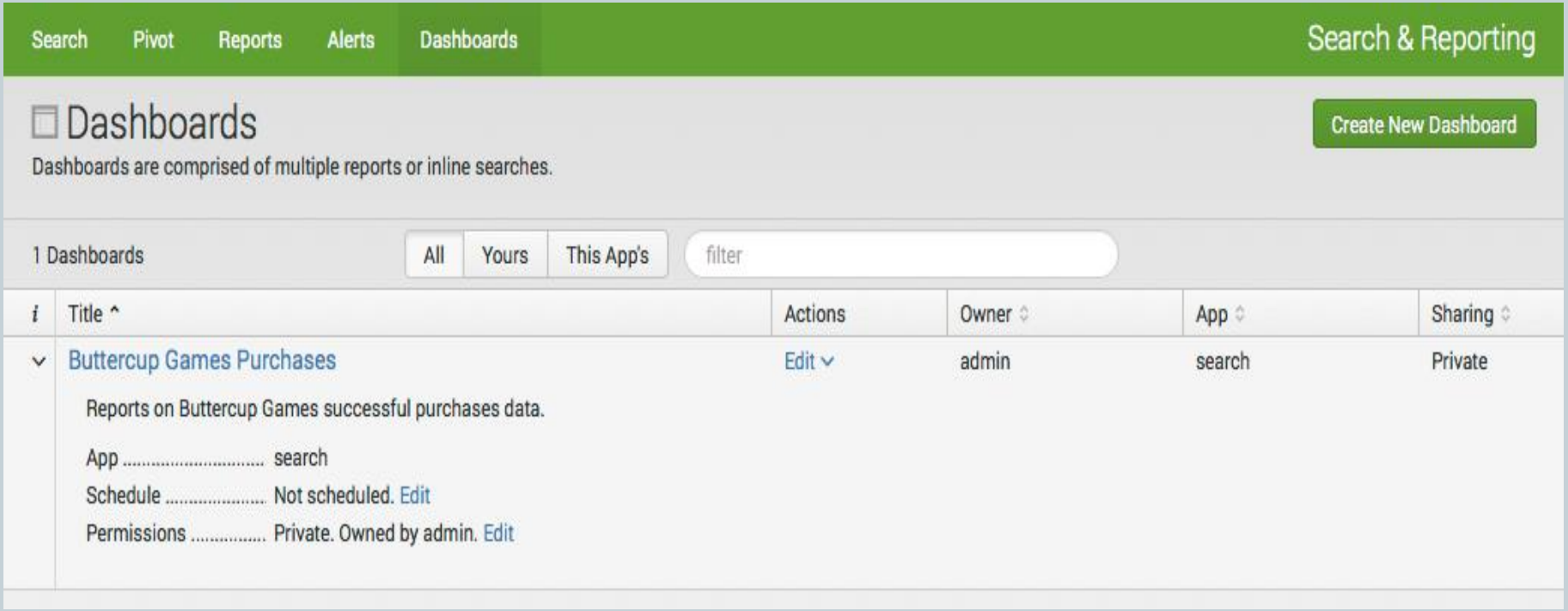
DASHBOARDS

2. Under the i column, click the arrow next to Buttercup Games Purchases to see more information about the dashboard: What app context it is in, whether or not it is scheduled, and its permissions.



DASHBOARDS

2. Under the i column, click the arrow next to Buttercup Games Purchases to see more information about the dashboard: What app context it is in, whether or not it is scheduled, and its permissions.



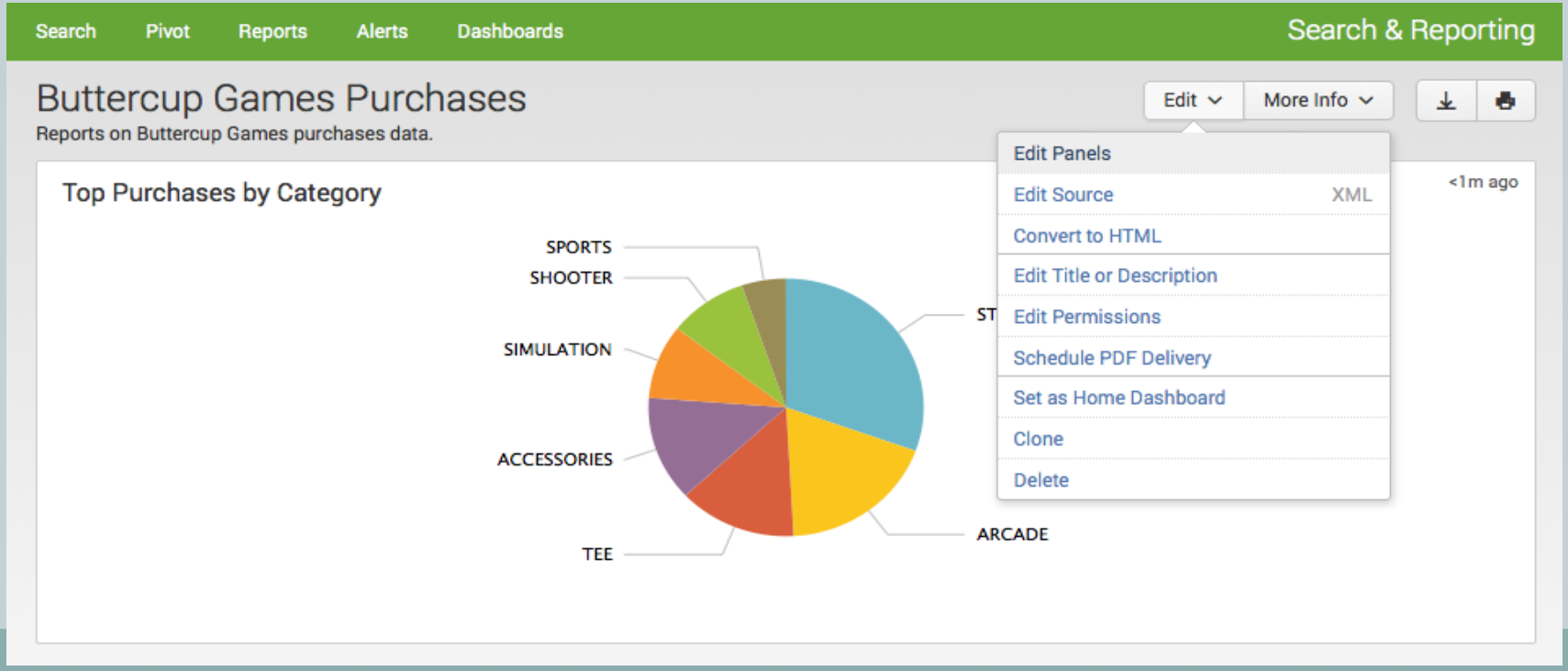
You can use the quick links that are inline with the information to edit the dashboard's Schedule and Permissions.

DASHBOARDS

- **Add an input to the dashboard**

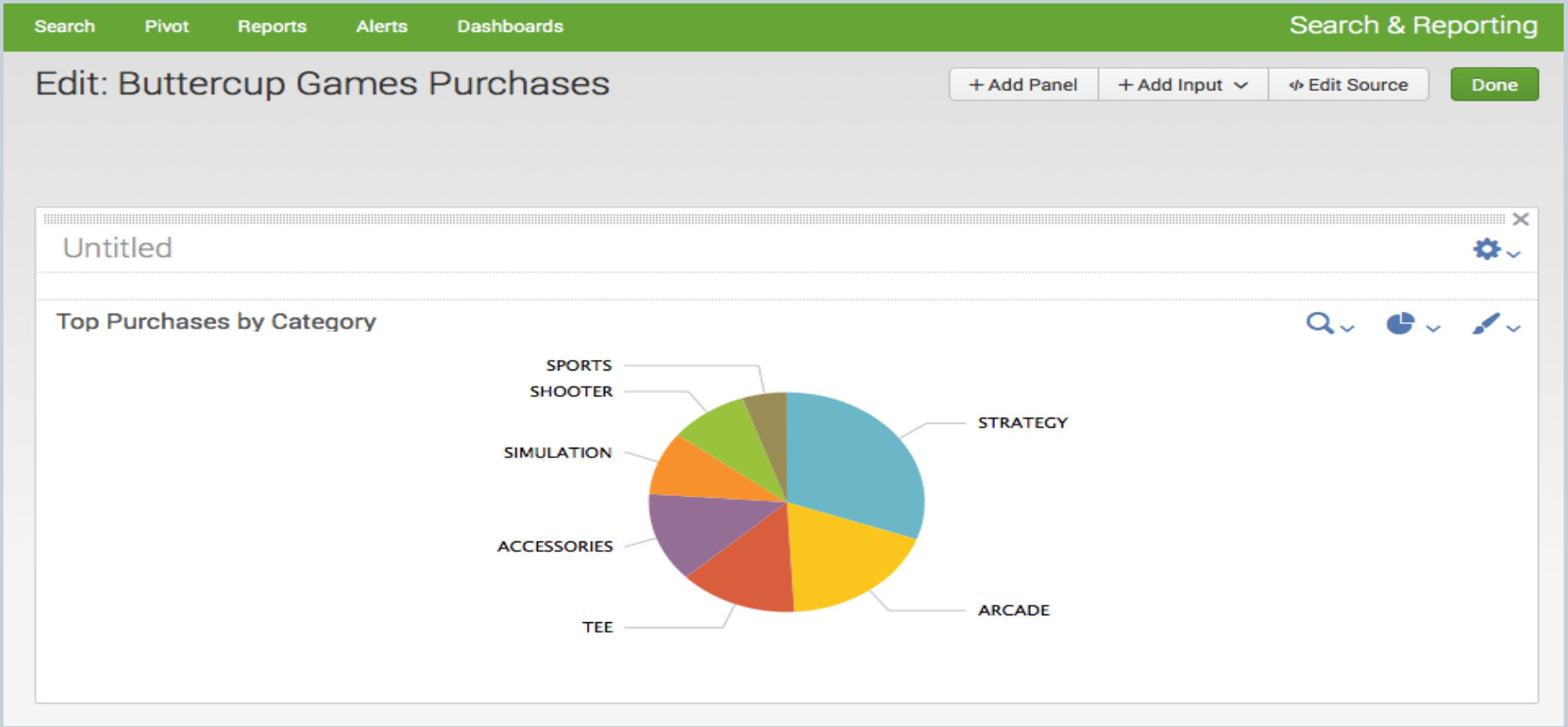
  1. In the Dashboards list, click Buttercup Games Purchases to return to the saved dashboard.

  2. Click Edit and select Edit Panels.



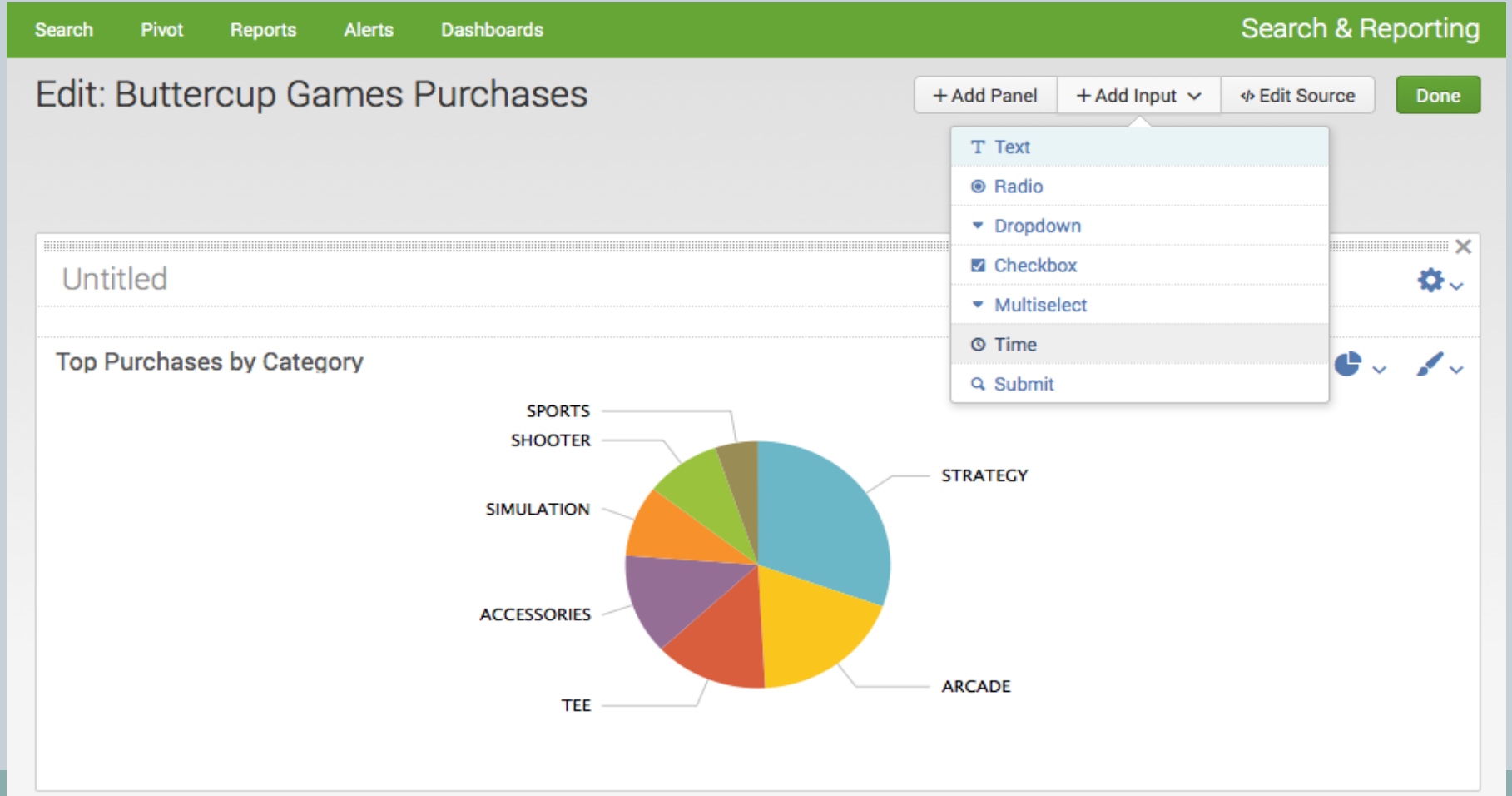
DASHBOARDS

- This changes the view so that edit options appear in the panels and modules on the dashboard.

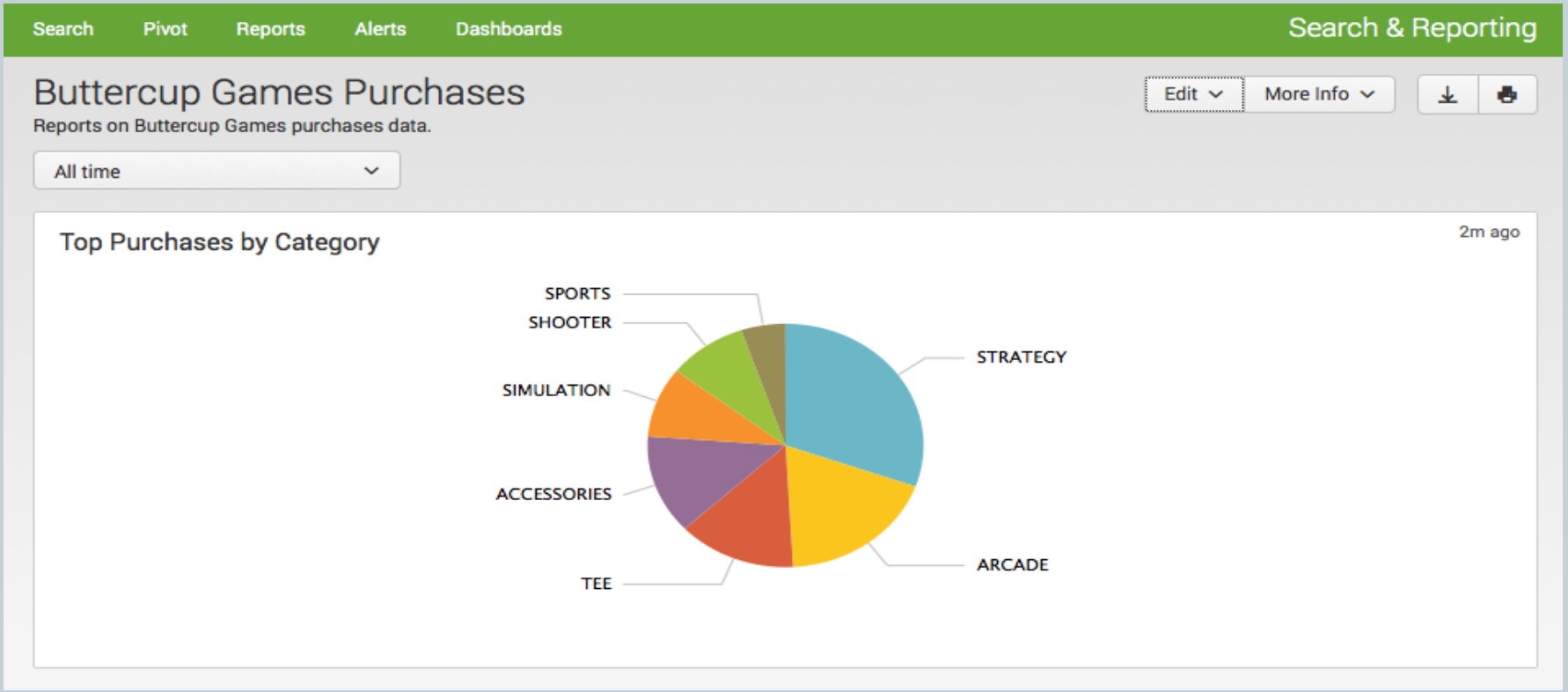


DASHBOARDS

- 3. Click Add Input and select Time.



- 4. Click Done.



- Now you can use this time range picker to restrict all the inline searches that power the panels to the same time range.

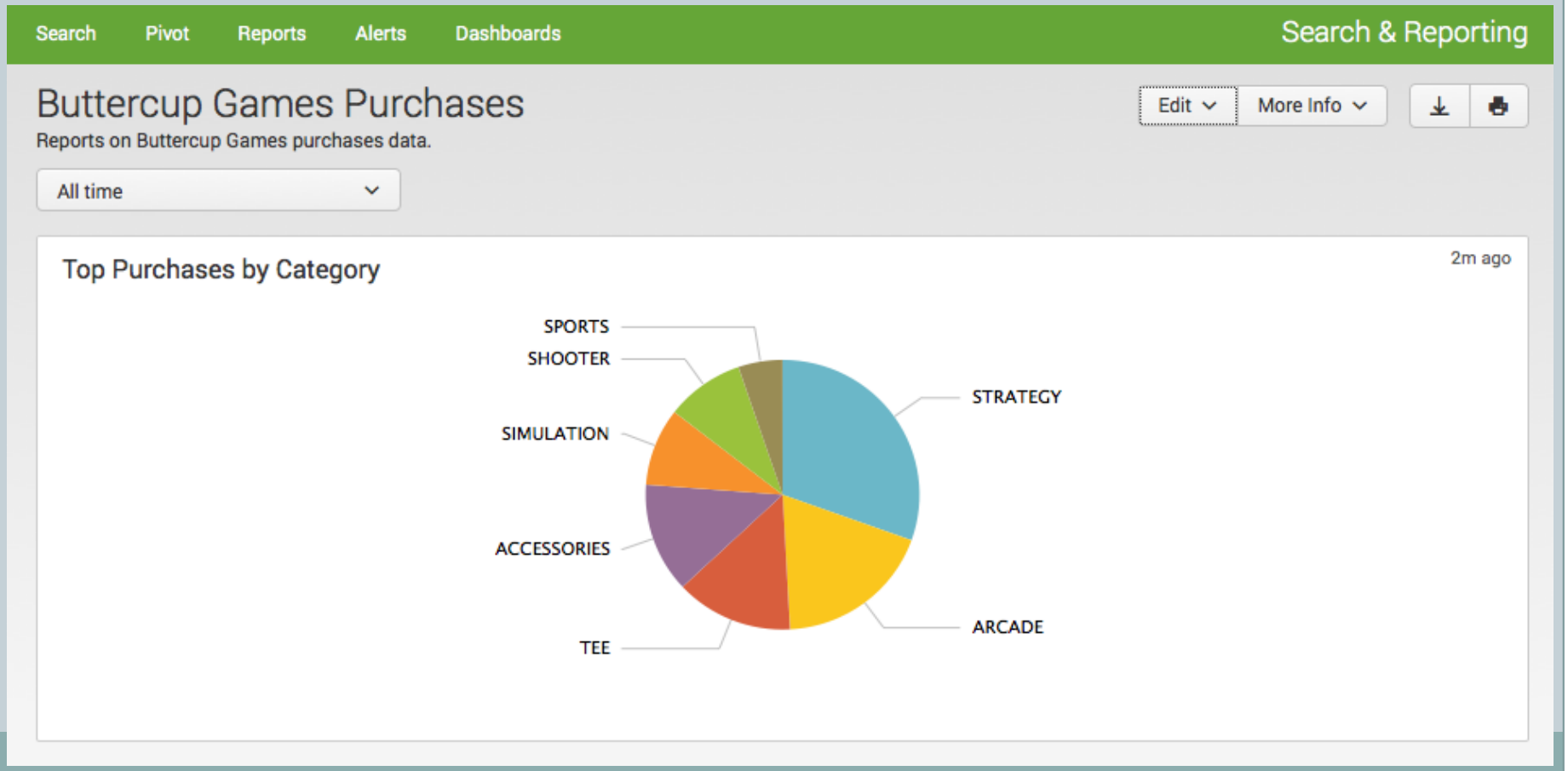
KOENIG
step forward

DASHBOARDS

Add more panels to the dashboard

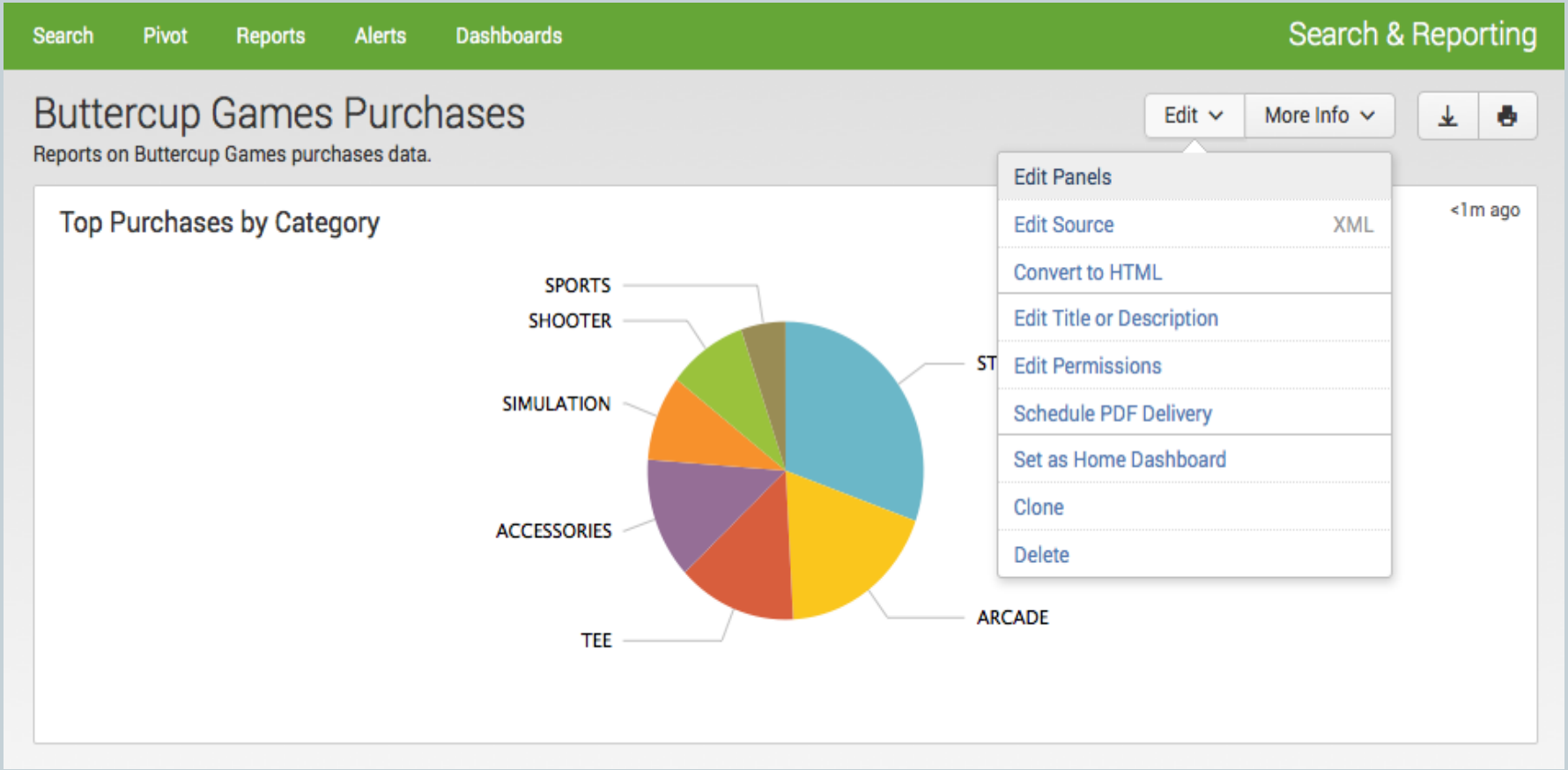
DASHBOARDS

- Add saved reports to the dashboard
- 1. Return to the Buttercup Games Purchases dashboard.



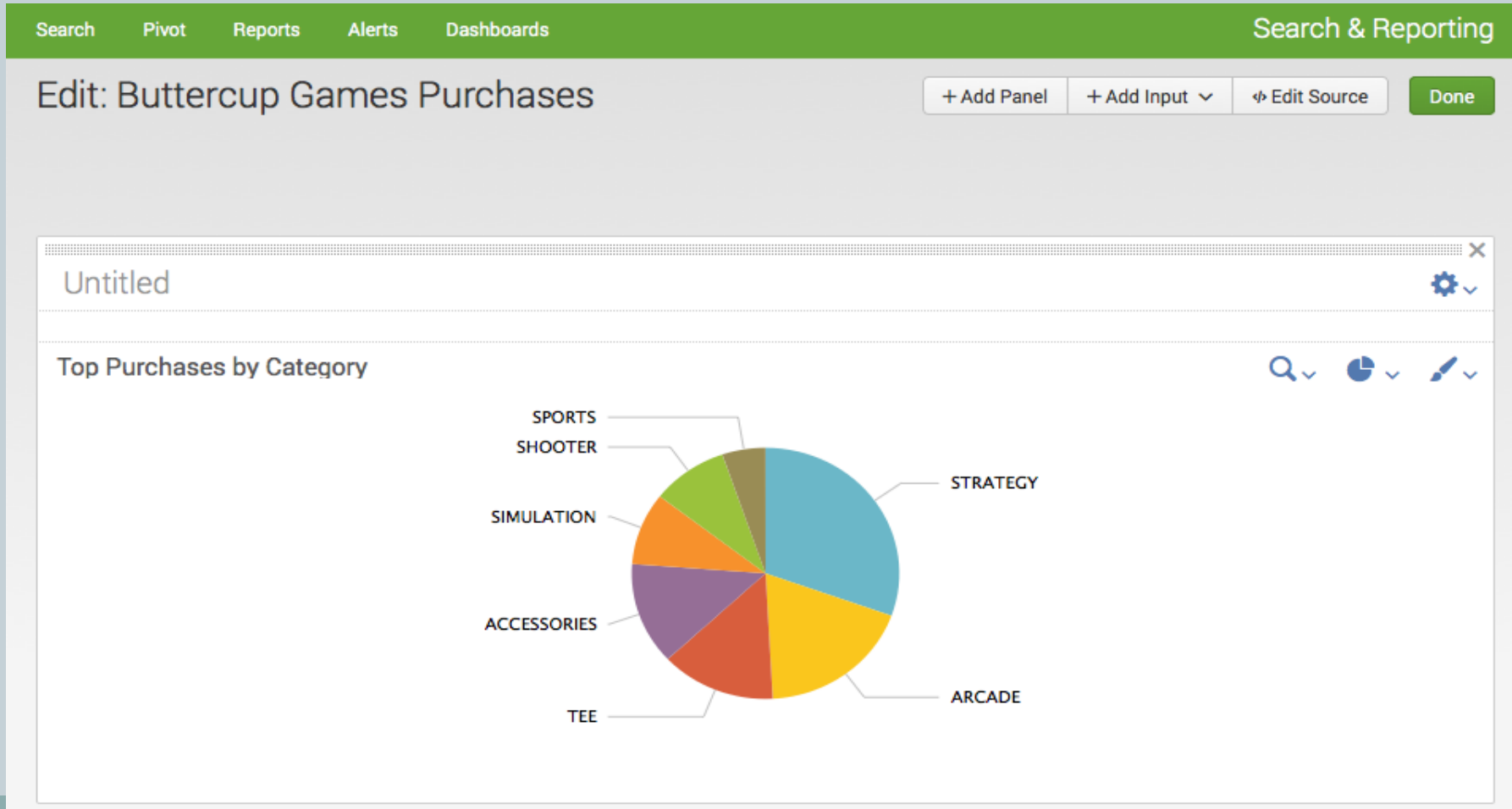
DASHBOARDS

- 2. Click Edit and select Edit Panels.



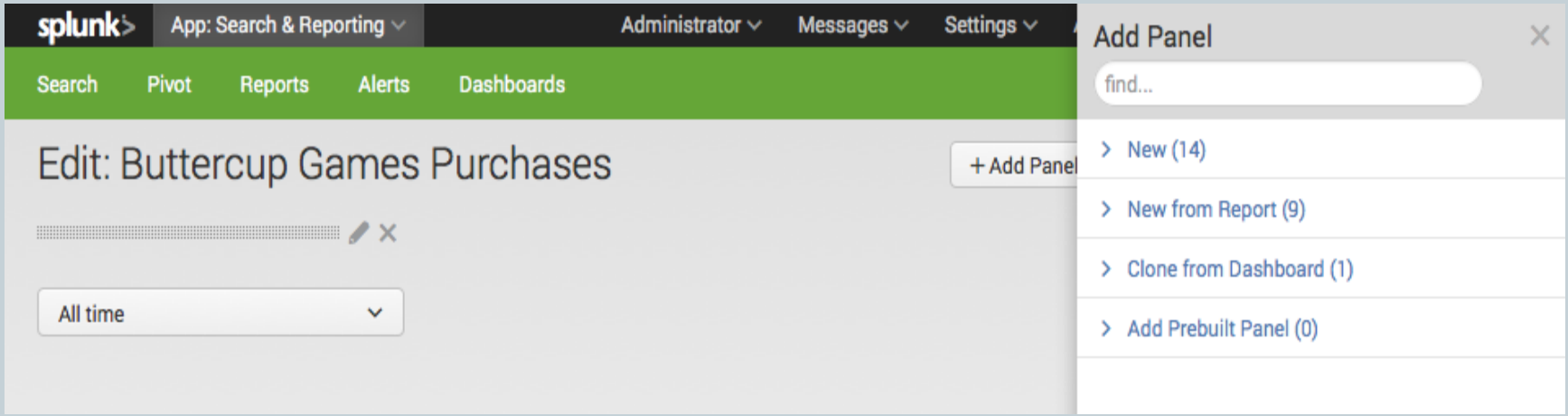
DASHBOARDS

- 3. In the Buttercup Games Purchases dashboard editor, click Add Panel.



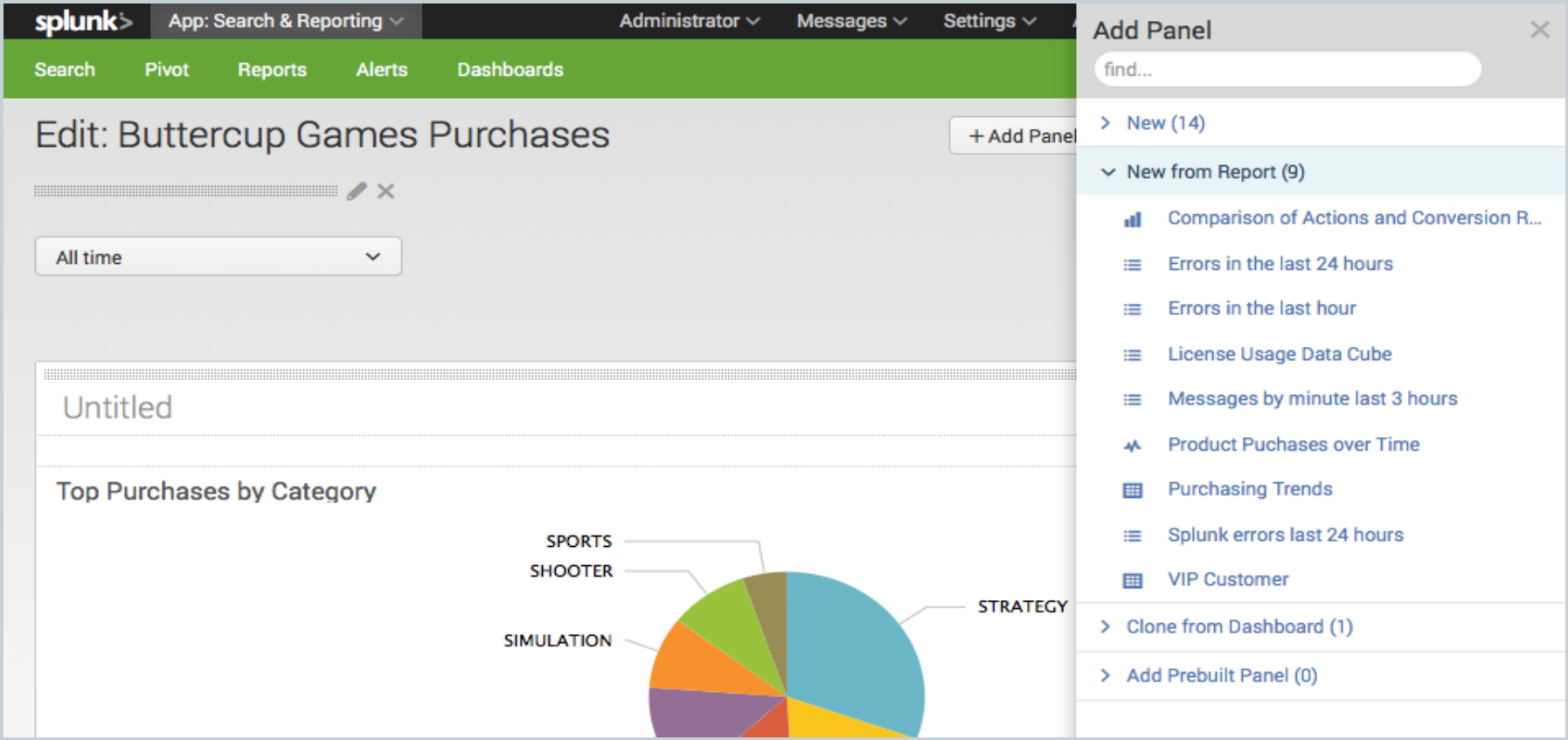
DASHBOARDS

- The Add Panel sidebar menu slides opens.



DASHBOARDS

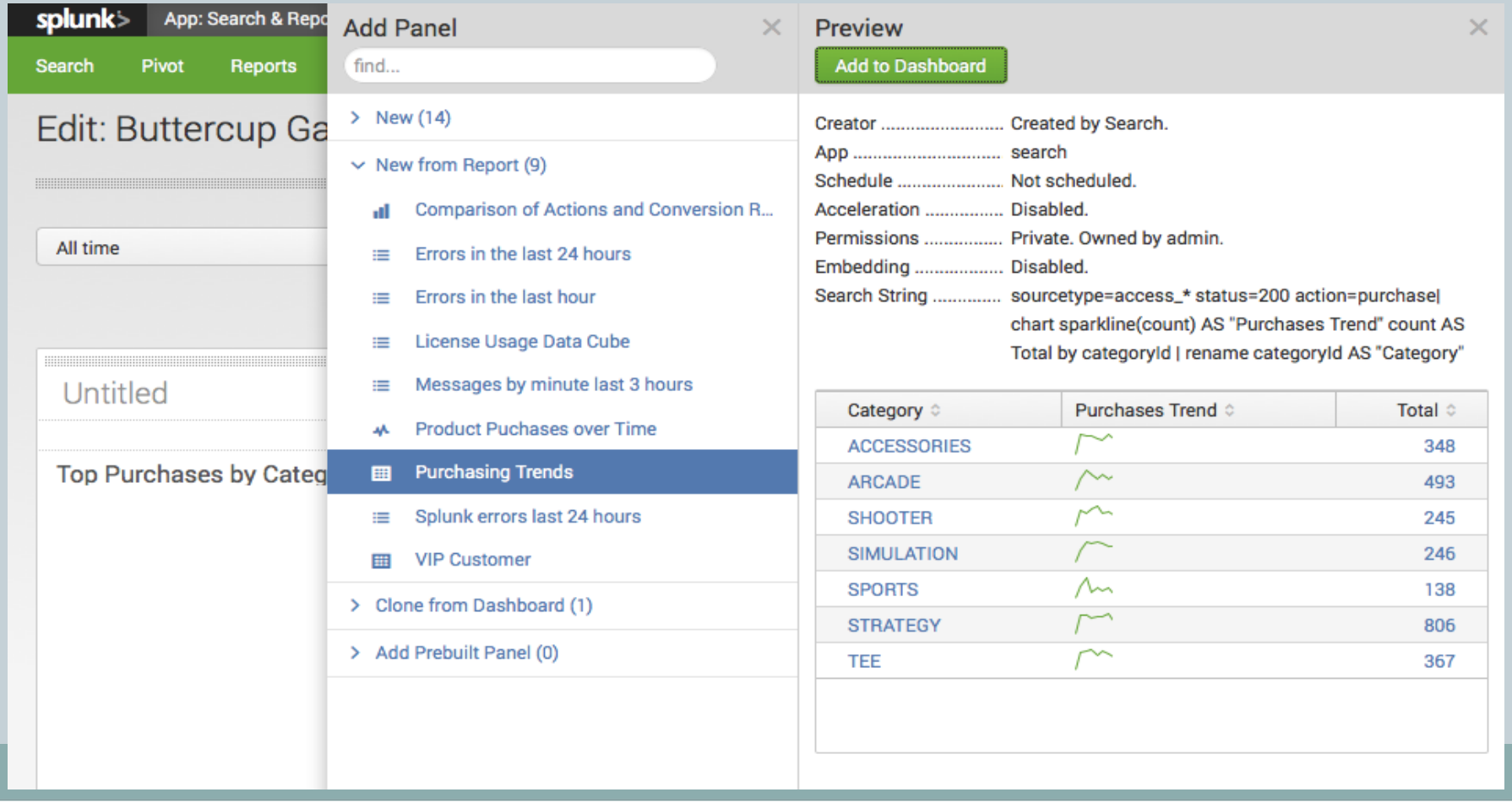
- 4. To add a new panel from a report, click New from Report.
- This opens the list of saved reports.



KOENIG
step forward

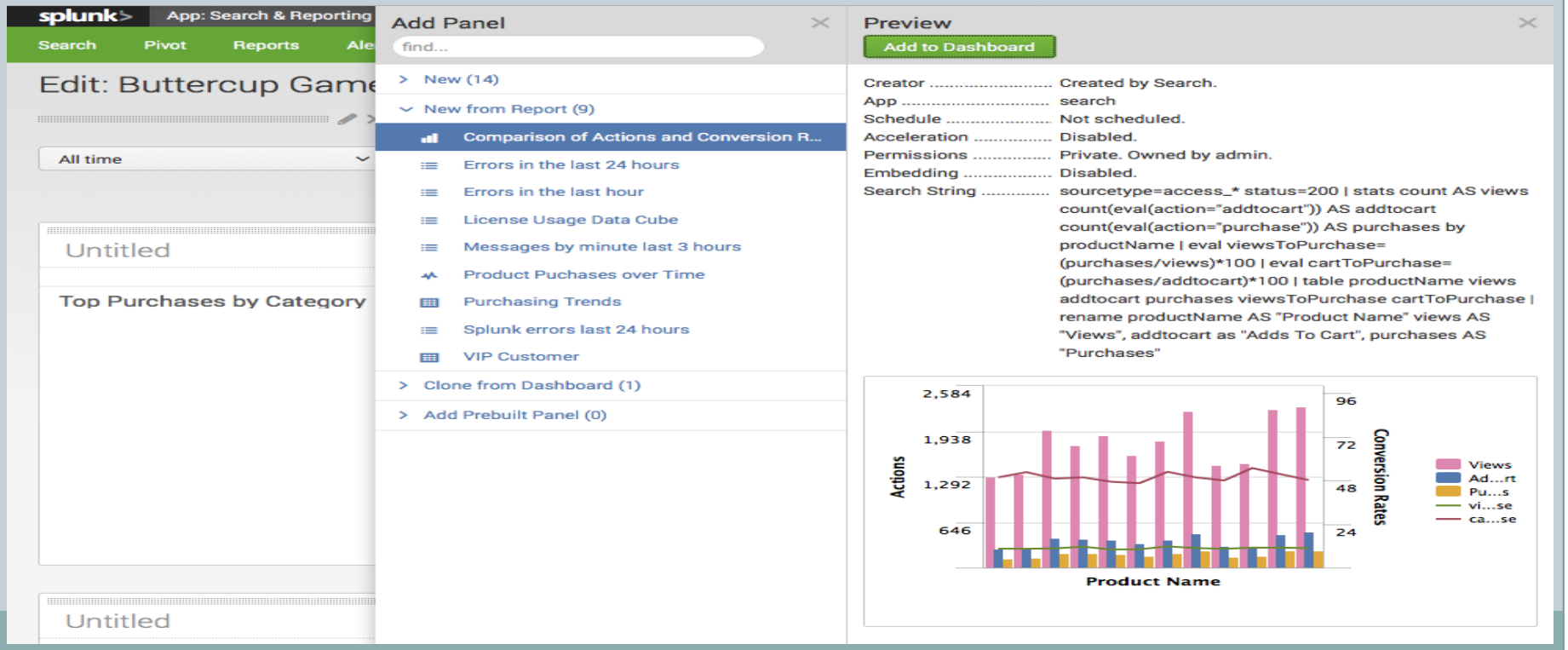
DASHBOARDS

- 5. Select Purchasing Trends.
- This opens a preview of the saved Report.



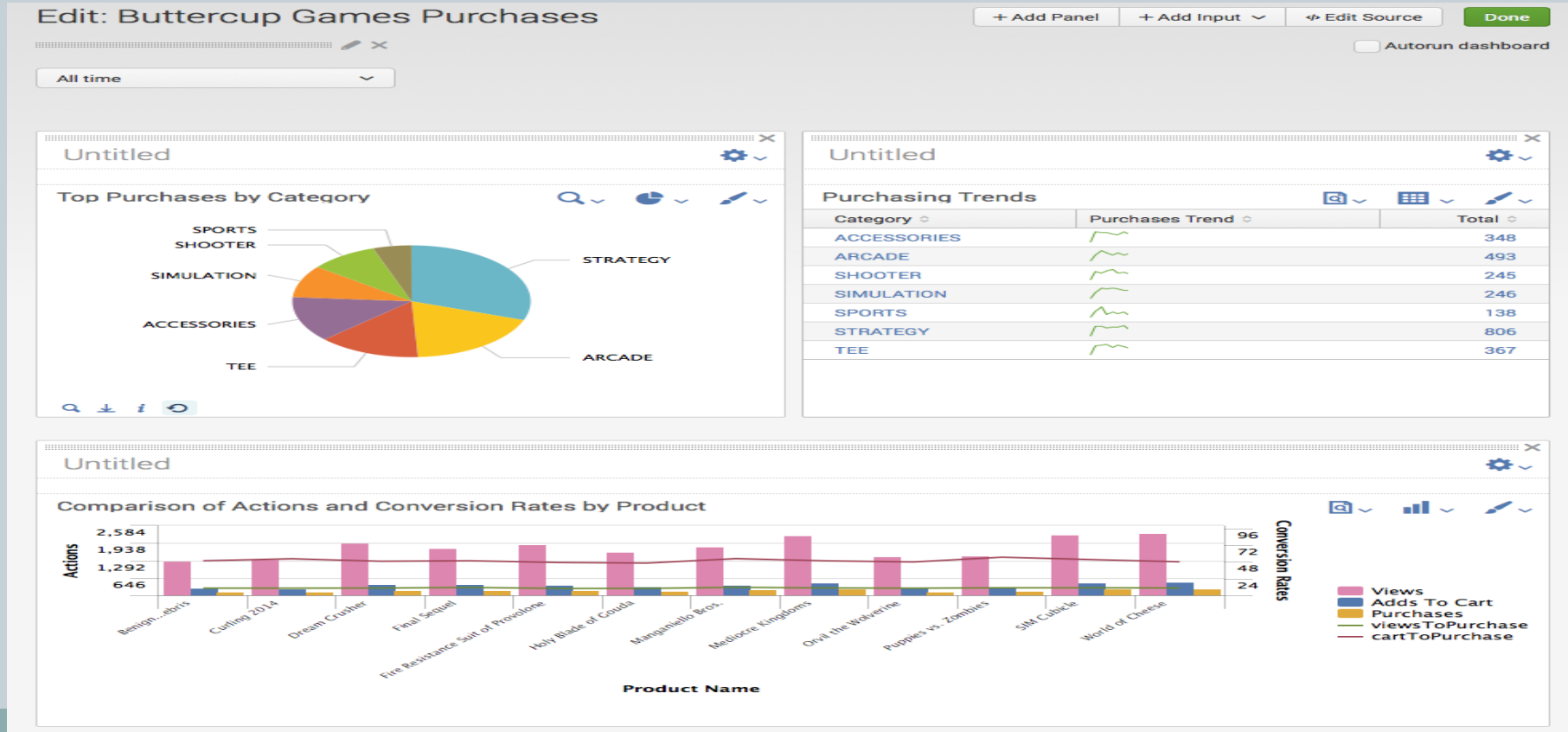
DASHBOARDS

- 6. Click Add to Dashboard.
- The new panel is placed in the dashboard editor. You can click anywhere to close the Add Panel sidebar menu or choose another report to add to the dashboard.
- 7. Select the report Comparison of Actions and Conversion Rates by Product and add it to the dashboard.



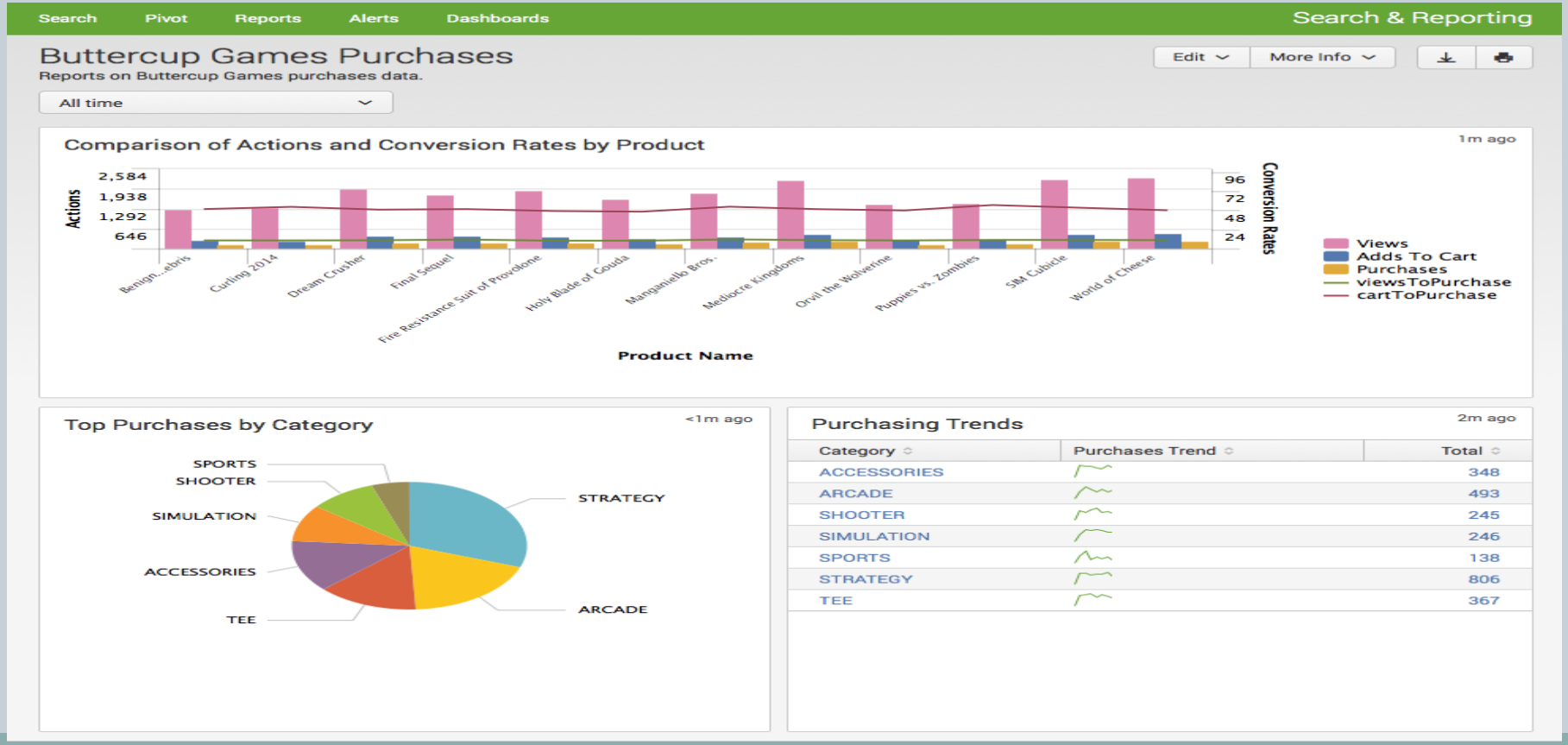
DASHBOARDS

- 8. Close the Add Panel sidebar and rearrange the panels on the dashboard.
- While in the dashboard editor, you can drag and drop a panel to rearrange it on the dashboard.



DASHBOARDS

- 9. Click Done.
- Your finished dashboard should look like this:



KOENIG
step forward

Deployment

- **Splunk Enterprise and your IT infrastructure**
- Splunk Enterprise indexes data from the servers, applications, databases, network devices, virtual machines, and so on, that make up your IT infrastructure. As long as the machine that generates the data is a part of your network, Splunk Enterprise can collect the data from machines located anywhere, whether it is local (on-the-premises in a server room), remote (off-the-premises in a datacenter), entirely in the cloud, or a hybrid (such as on-premise and in the cloud).
- Most users connect to Splunk Enterprise with a web browser and use Splunk Web to administer their deployment, manage and create knowledge objects, run searches, create pivots and reports, and so on. You can also use the command-line interface to administer your Splunk Enterprise deployment.

KOENIG
step forward

Splunk Enterprise Components

Component	Description
Apps	Apps are a collection of configurations, knowledge objects, and customer designed views and dashboards that extend the Splunk Enterprise environment to fit the specific needs of organizational teams such as Unix or Windows system administrators, network security specialists, website managers, business analysts, and so on. A single Splunk Enterprise installation can run multiple apps simultaneously.
Forwarder	A forwarder is a Splunk Enterprise instance that forwards data to another Splunk Enterprise instance (an indexer or another forwarder) or to a third-party system.
Indexer	An indexer is the Splunk Enterprise instance that indexes data. The indexer transforms the raw data into events and stores the events into an index. The indexer also searches the indexed data in response to search requests.
Receiver	A receiver is a Splunk Enterprise instance configured to receive data from a forwarder. The receiver is either an indexer or another forwarder.
Search head	In a distributed search environment, the search head is the Splunk Enterprise instance that handles search management functions, directing search requests to a set of search peers and then merging the results back to the user. If this instance does only searching and not indexing, it is usually referred to as a dedicated search head.
Search peer	In a distributed search environment, the search peer is the Splunk Enterprise instance that performs indexing and fulfills search requests originating from the search head.