



Splunk Fundamentals 1

Outline

- Module 1-2: Introducing Splunk and Splunk's Components
- Module 3: Installation
- Module 4: Inputs
- Module 5: Searching
- Module 6: Using Fields in Searches
- Module 7: Best Practices for Searching
- Module 8: Splunk's Search Language
- Module 9: Transforming Commands
- Module 10: Creating Reports and Dashboards
- Module 11: Using Pivot
- Module 12: Creating and Using Lookups
- Module 13: Creating Scheduled Reports and Alerts

Modules 1-2: Introducing Splunk and Splunk's Components

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module Objectives

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

Got Data?

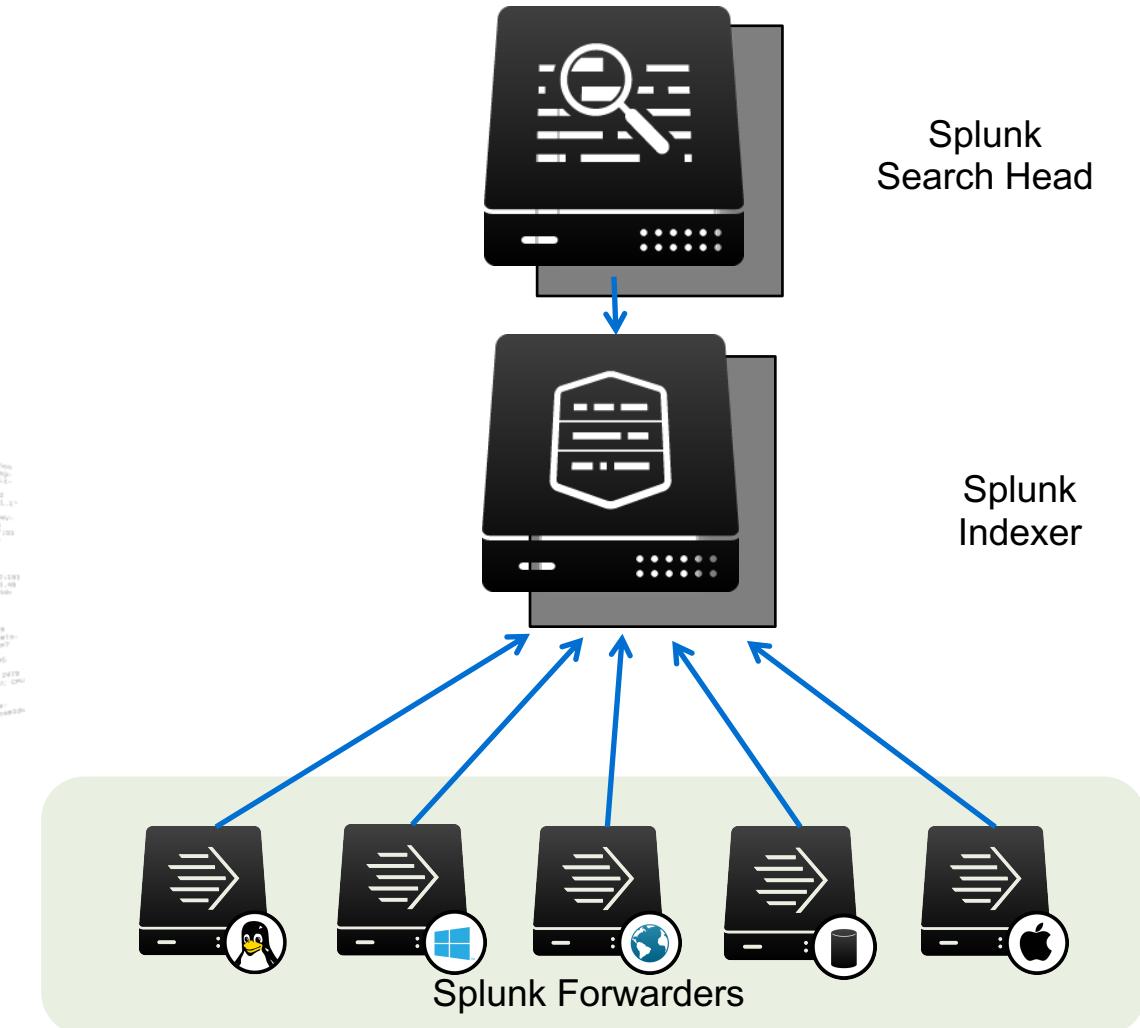


- Computers
- Network devices
- Virtual machines
- Internet devices
- Communication devices
- Sensors
- Databases
- **Any source**



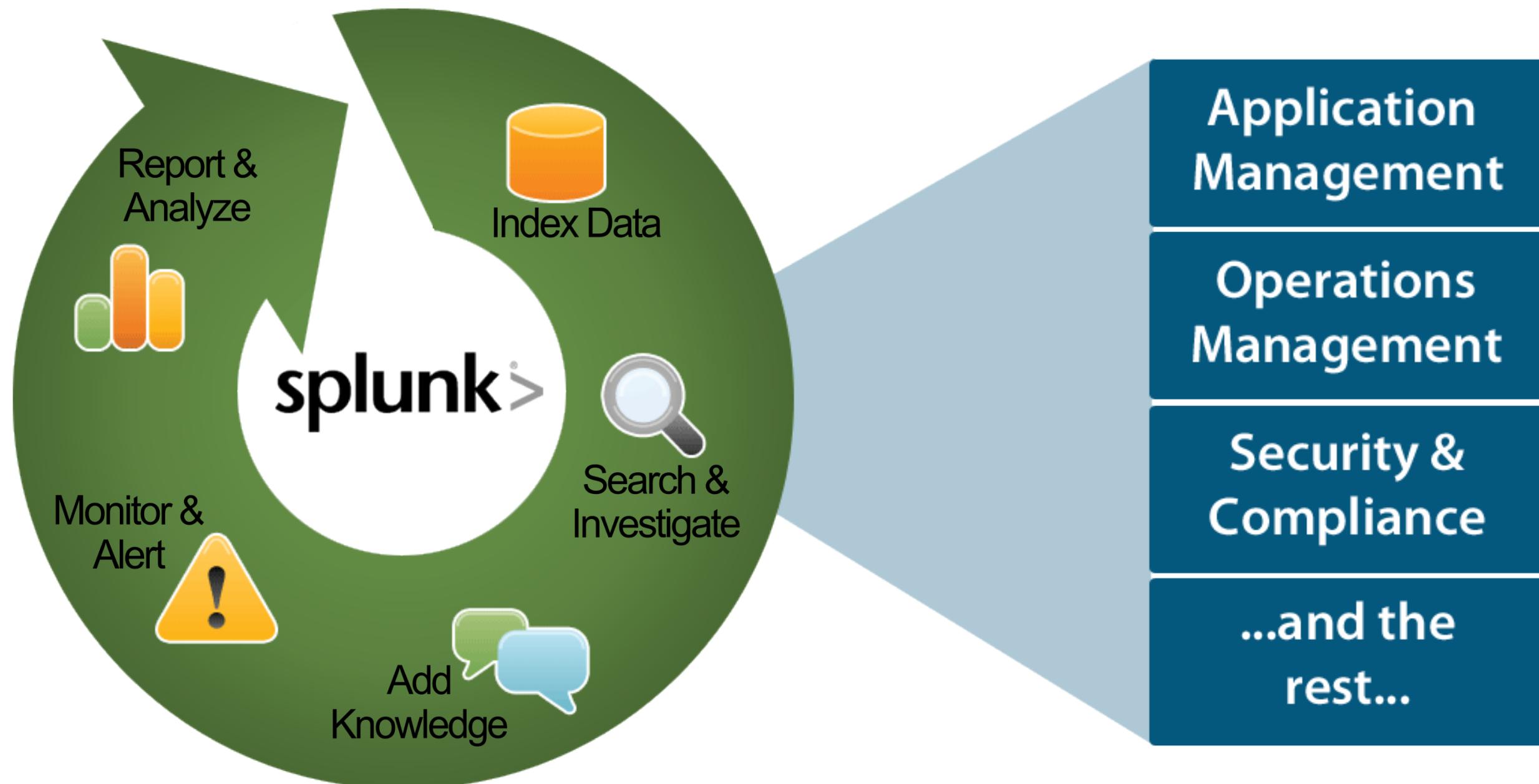
- Logs
- Configurations
- Messages
- Call detail records
- Clickstream
- Alerts
- Metrics
- Scripts
- Changes
- Tickets
- **Any data**

Users Searching



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

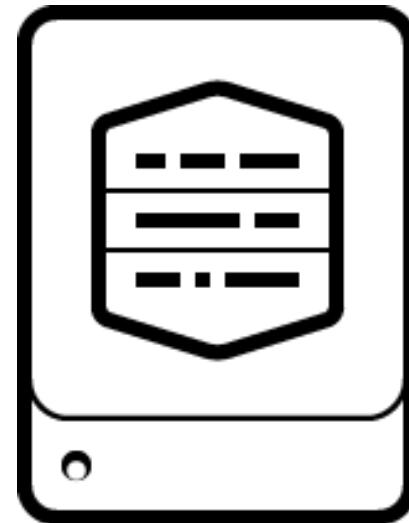
One Splunk. Many Uses.



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Splunk Components

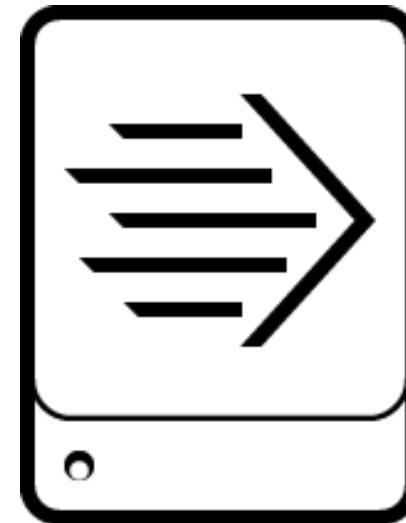
- Splunk is comprised of three main processing components:



Indexer



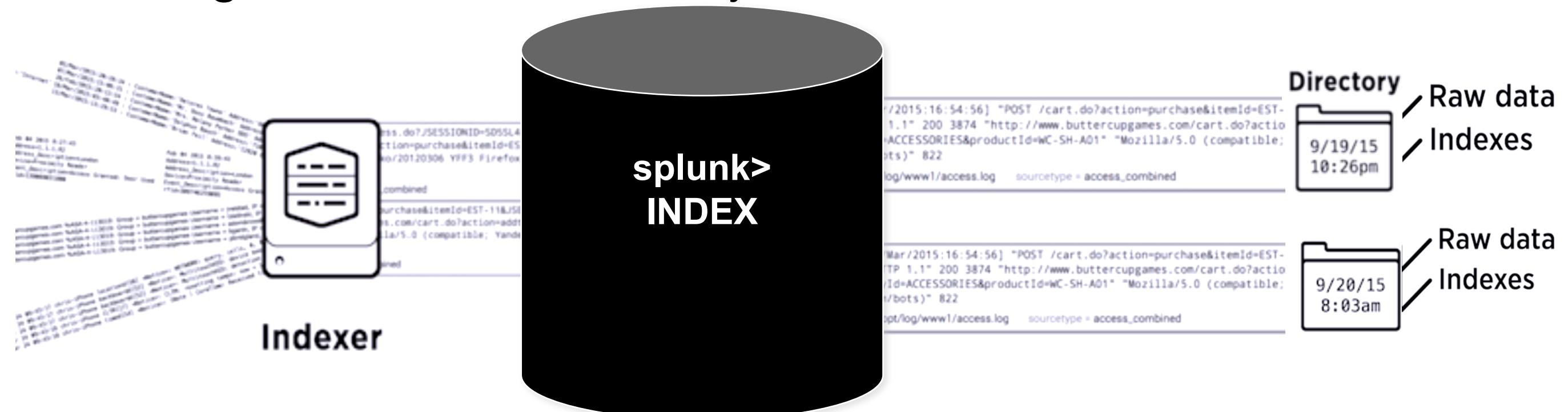
Search Head



Forwarder

Splunk Components - Indexer

- Processes machine data, storing the results in Indexes as events, enabling fast search and analysis

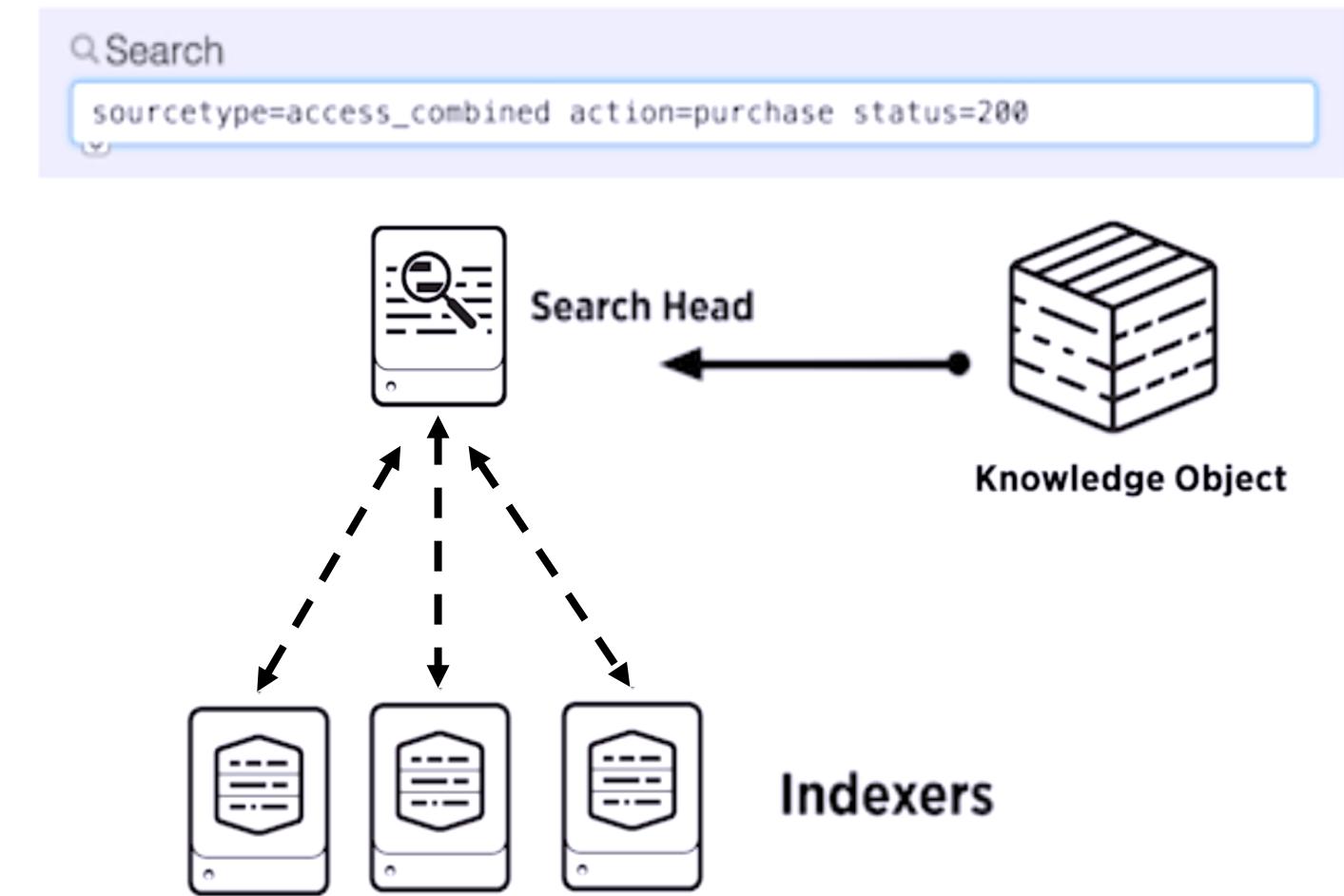


- As the Indexer indexes data, it creates a number of files organized in sets of directories by age
 - Contains raw data (compressed) and Indexes (points to the raw data)

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Splunk Components – Search Heads

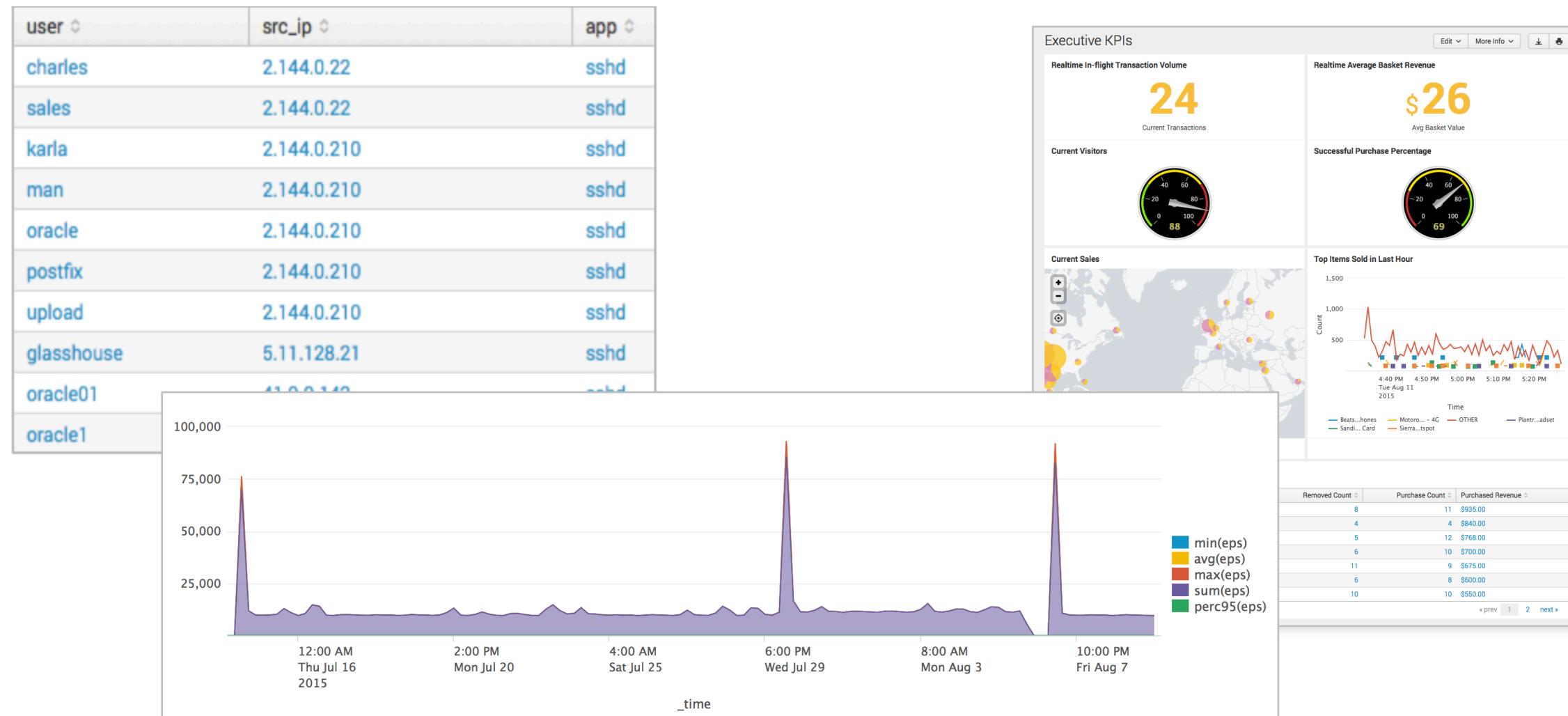
- Allows users to use the Search language to search the indexed data
- Distributes user search requests to the Indexers
- Consolidates the results and extract field value pairs from the events to the user
- Knowledge Objects on the Search Heads can be created to extract additional fields and transform the data without changing the underlying Index data



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Splunk Components – Search Heads (cont.)

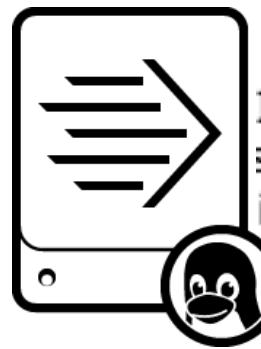
- Search Heads also provide tools to enhance the search experience such as reports, dashboards and visualizations



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Splunk Components – Forwarders

- Splunk Enterprise instances that consume and send data to the index
- Require minimal resources and have little impact on performance
- Typically reside on the machines where the data originates
- Primary way data is supplied for indexing



**Web Server
with Forwarder Instance
installed**

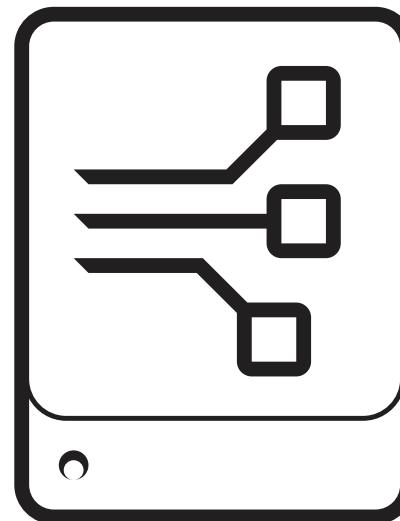
IP = 10.3.10.6, Session disconnected. Session type = TPsecOve
IP = 10.1.10.216, Session connected. Session type = SSL, Dura
s, IP = 10.1.10.133, Session connected. Session type = IKE, Dur
i, IP = 10.3.10.18, Session disconnected. Session type = IKE, D
= 10.1.10.211, Session connected. Session type = SSL, Duration



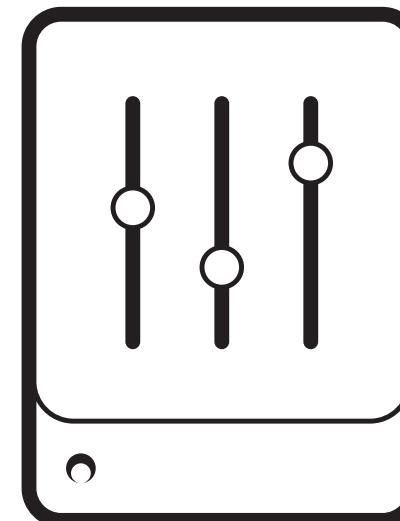
Indexer

Additional Splunk Components

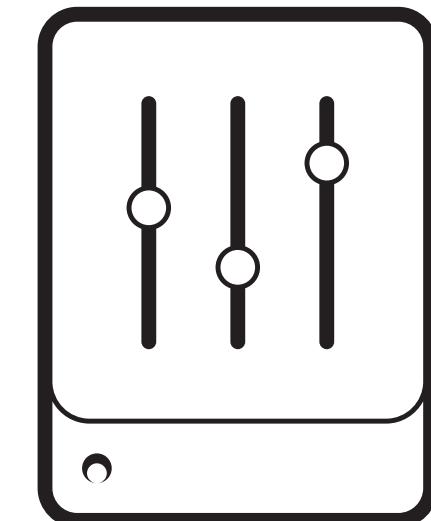
- In addition to the three main Splunk processing components, there are some less-common components including :



**Deployment
Server**



Cluster Master

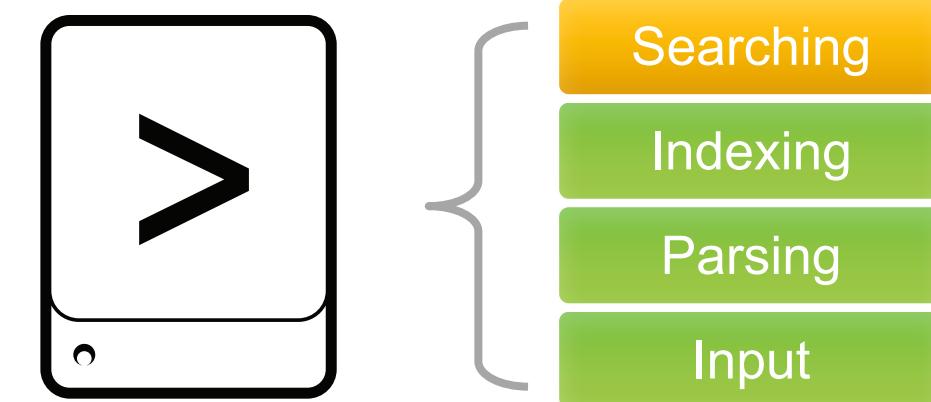


License Master

Splunk Deployment – Standalone

- **Single Server**

- All functions in a single instance of Splunk
- For testing, proof of concept, personal use, and learning
- This is what you get when you download Splunk and install with default settings



- Recommendation

- Have at least one test/development setup at your site

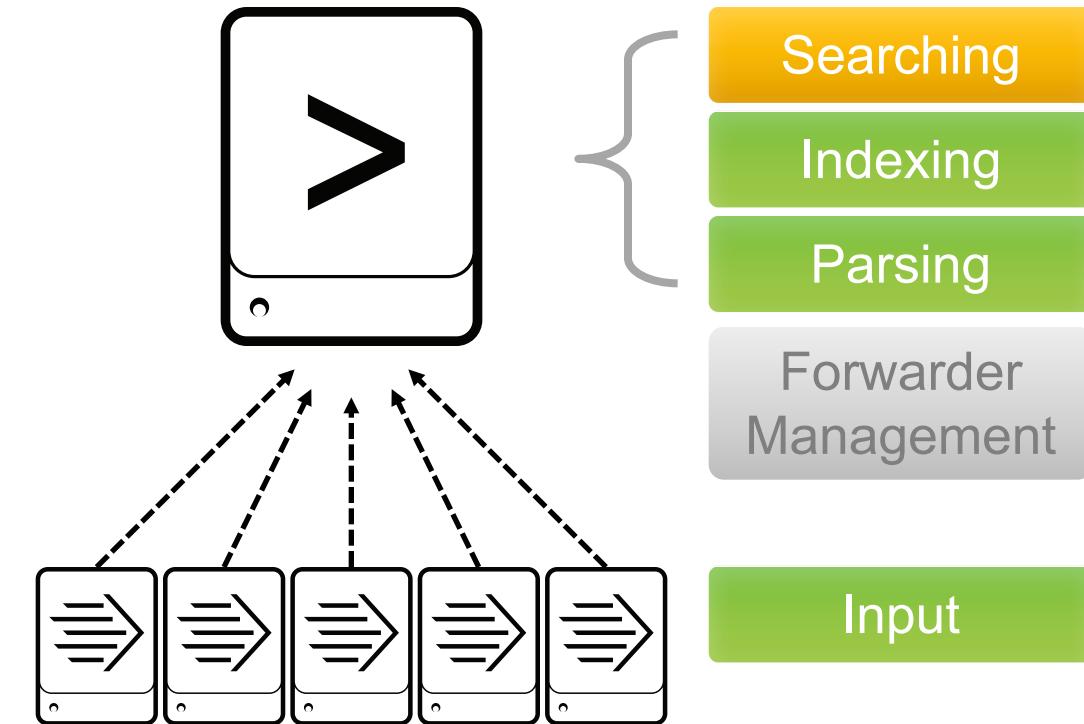
Splunk Deployment – Basic

- **Splunk server**

- Similar to server in standalone configuration
- Manage deployment of forwarder configurations

- **Forwarders**

- Forwarders collect data and send it to Splunk servers
- Install forwarders at data source (usually production servers)

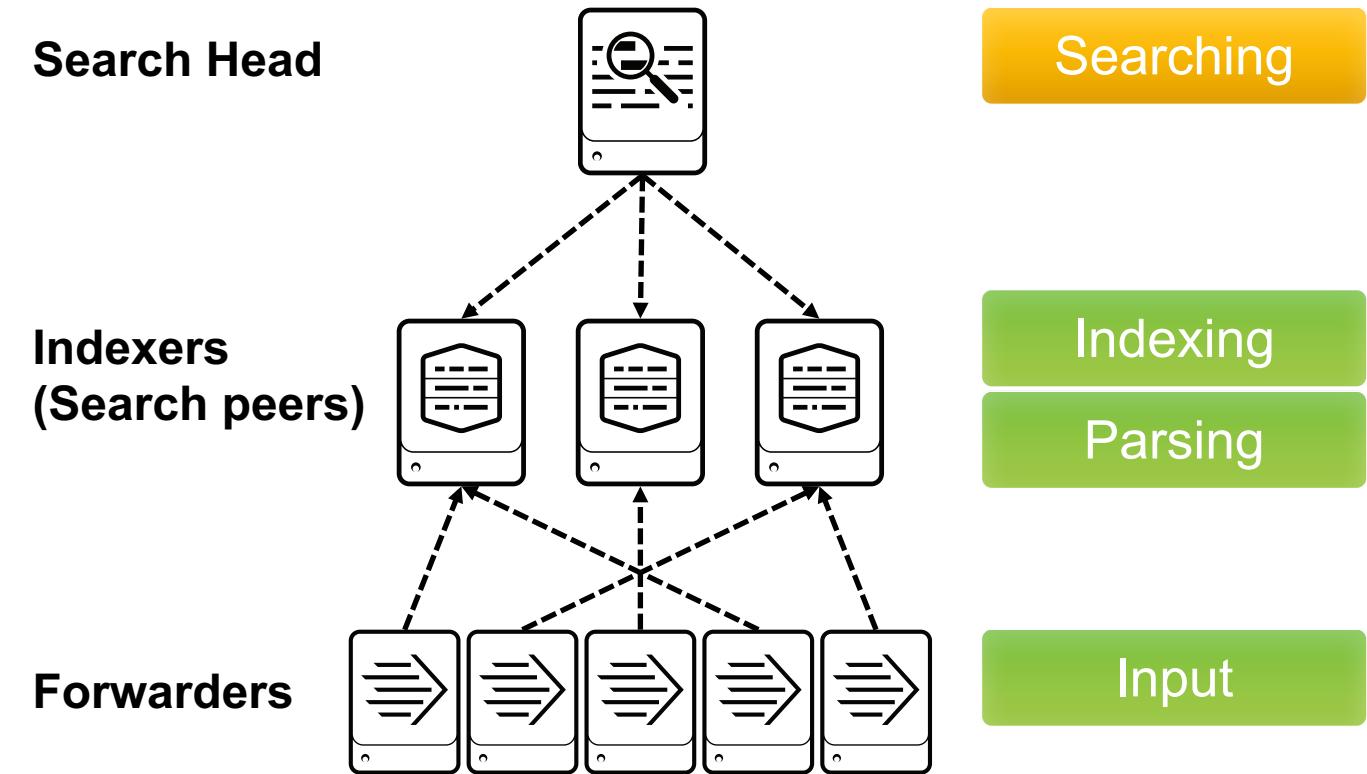


Basic Deployment for organizations:

- Indexing less than 20GB per day
- With under 20 users
- Small amount of forwarders

Splunk Deployment – Multi-Instance

- Increases indexing and searching capacity
- Search management and index functions are split across multiple machines

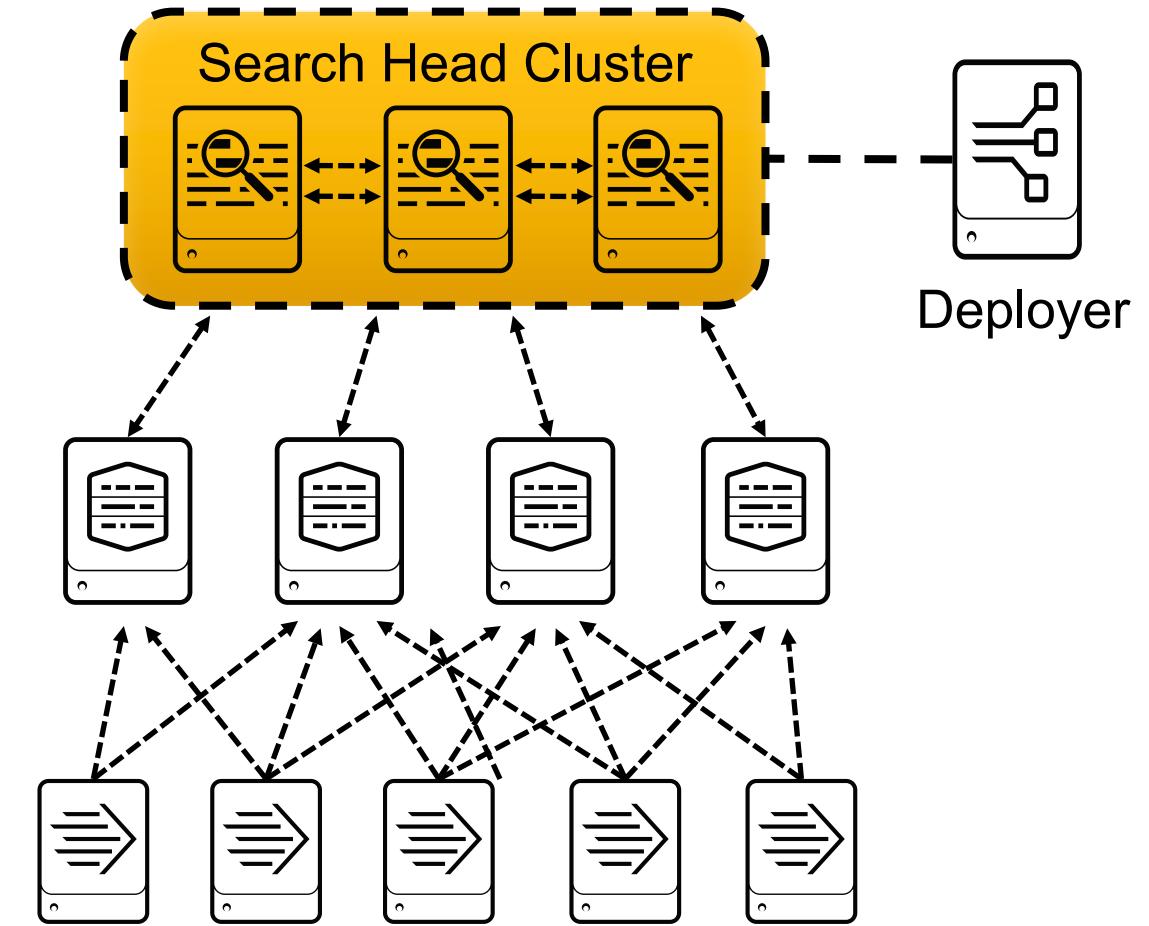


Deployment for organizations:

- Indexing up to 100 GB per day
- Supports 100 users
- Supports several hundred forwarders

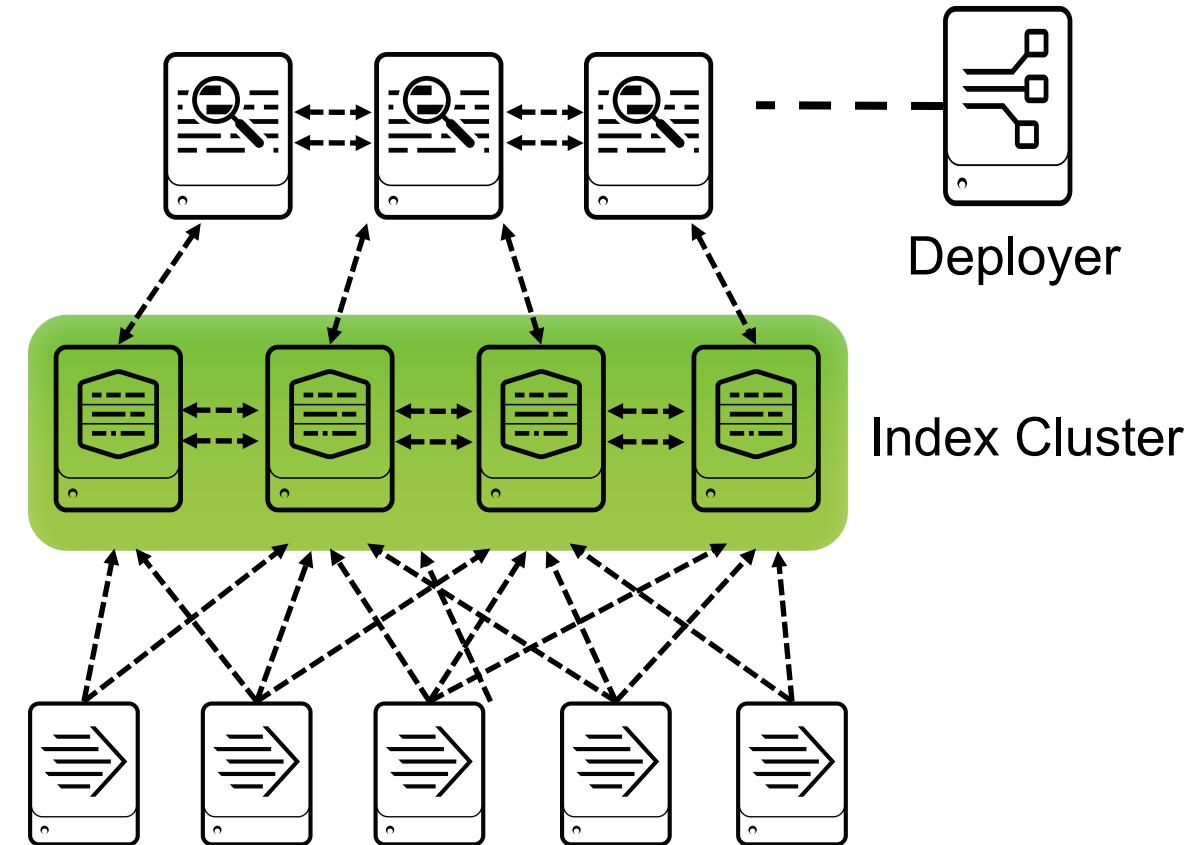
Splunk Deployment – Increasing Capacity

- Adding a Search Head Cluster:
 - services more users for increased search capacity
 - allows users and searches to share resources
 - Coordinate their activities to handle search requests and distribute the requests across the set of indexers
- Search Head Clusters require a minimum of three Search Heads
- A Deployer is used to manage and distribute apps to the members of the Search Head Cluster



Splunk Deployment – Index Cluster

- Traditional Index Clusters:
 - Configured to replicate data
 - Prevent data loss
 - Promote availability
 - Manage multiple indexers
- Non-replicating Index Clusters
 - Offer simplified management
 - Do not provide availability or data recovery



Module 3: Installation

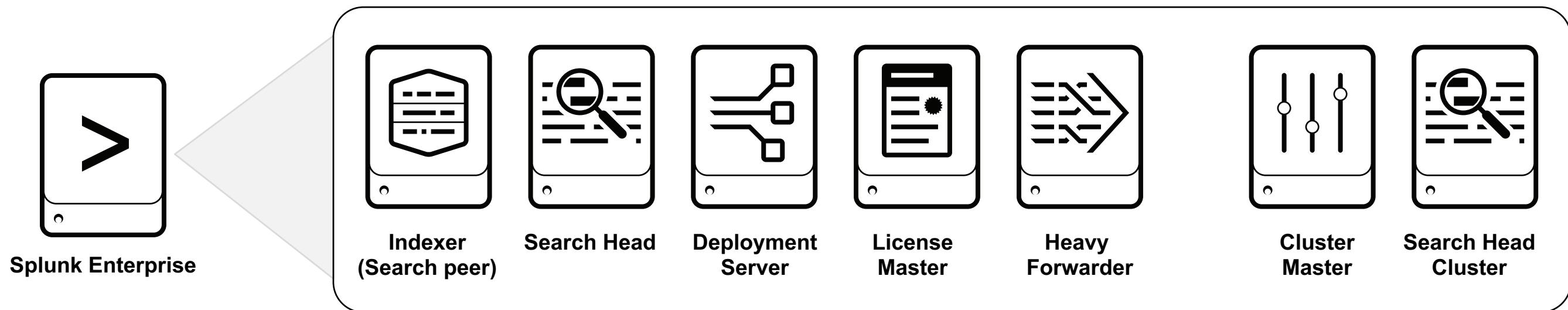
Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module Objectives

- Describe Splunk installation
- Describe Splunk component installation
- Using Splunk Web Admin
- Identify common Splunk commands
- Identify Splunk directory structure

Splunk Enterprise Install Package

- There are multiple Splunk components installed from the Splunk Enterprise package:



Splunk Enterprise Installation Overview

- Verify required ports are open (splunkweb, splunkd, forwarder) and start-up account
- Download Splunk Enterprise from www.splunk.com/download
- Installation: (as account running Splunk)
 - ***NIX** – un-compress the **.tar.gz** file in the path you want Splunk to run from
 - **Windows** – execute the **.msi** installer and follow the wizard steps
- Complete installation instructions at:
docs.splunk.com/Documentation/Splunk/latest/Installation/Chooseyourplatform
- After installation:
 - Splunk starts automatically on Windows
 - Splunk must be manually started on ***NIX** until **boot-start** is enabled

Splunk Component Installation Overview

- Installing Splunk Enterprise as an Indexer or Search Head is identical to installing a single deployment instance
- The difference happens at a configuration level
 - Installation as configuration is an iterative and ongoing event as you build and scale your deployment
 - Administrators need to be in control of the environment to fulfill emerging needs
 - Before installing Indexers or Search Heads, be sure to keep in mind the different hardware requirements

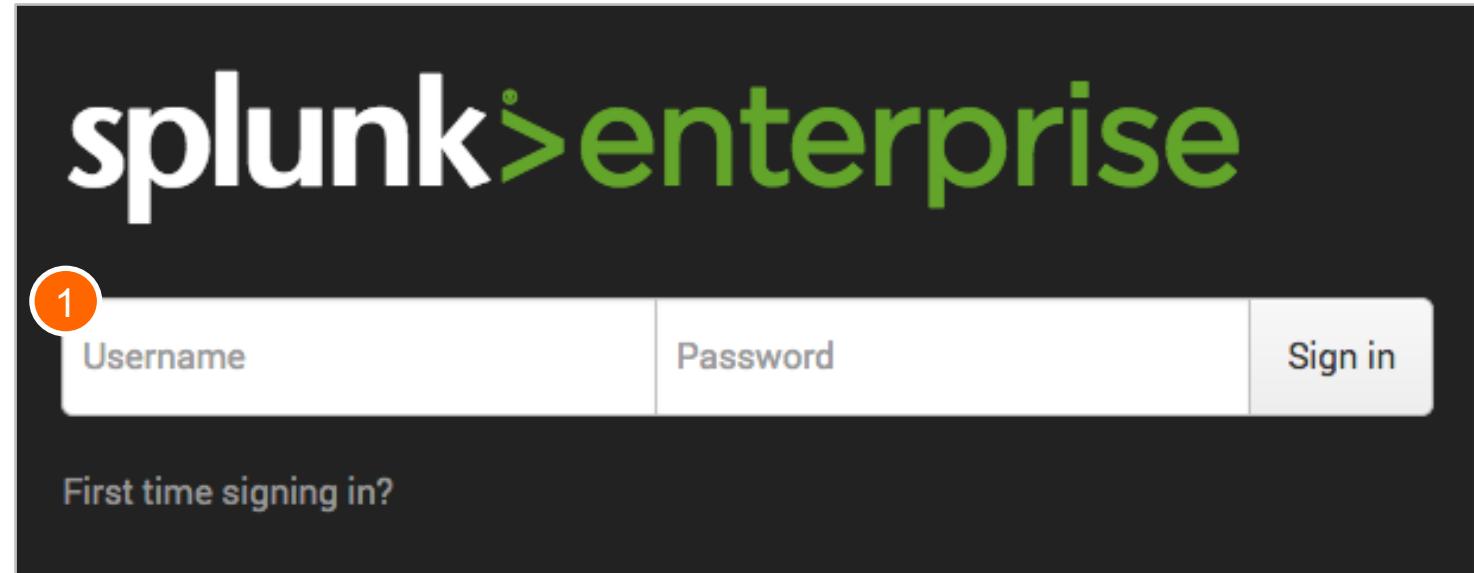
Common Splunk Commands

- **splunk** is the program in the **bin** directory to run the CLI

Command	Operation
splunk help	Display a usage summary
splunk [start stop restart]	Manages the Splunk processes
splunk start --accept-license	Automatically accept the license without prompt
splunk status	Display the Splunk process status
splunk show splunkd-port	Show the port that the splunkd listens on
splunk show web-port	Show the port that Splunk Web listens on
splunk show servername	Show the servername of this instance
splunk show default-hostname	Show the default host name used for all data inputs
splunk enable boot-start -user	Initialize script to run Splunk Enterprise at system startup

Logging In

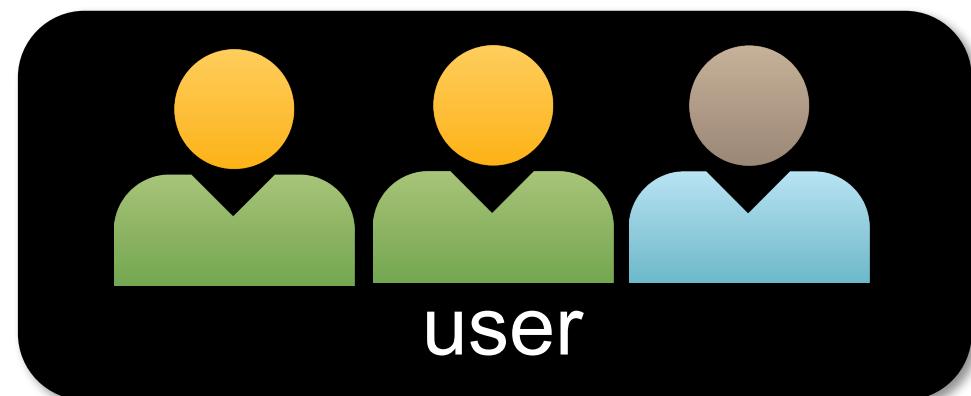
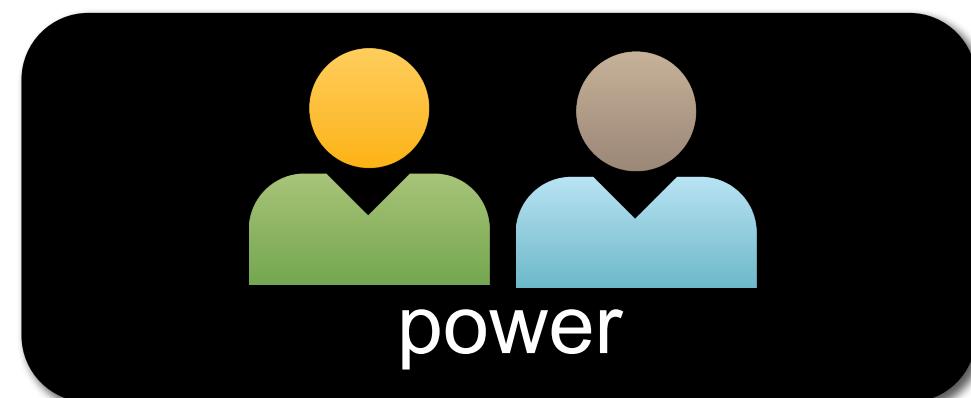
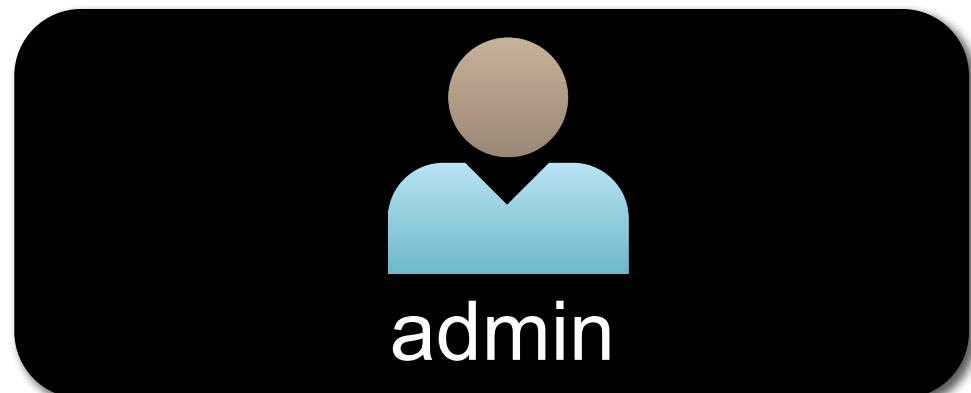
- ① Log in to Splunk with a web browser
- ② Based on your default app, its main view appears
 - The Home view is shown here
 - You or your organization may change your default app



The image shows the Splunk Enterprise home screen for the "Search & Reporting" app. The top navigation bar includes the Splunk logo, user information (student16), and various menu options like Messages, Settings, Activity, Help, and Find. A "Apps" dropdown is open, showing the "Search & Reporting" app as the active choice. The main content area is titled "Explore Splunk Enterprise" and features three circular icons with corresponding manuals: "Search Manual" (with a magnifying glass icon), "Pivot Manual" (with a chart icon), and "Dashboards & Visualizations" (with a bar chart icon). Below each manual is a brief description. At the bottom of the screen, the text "Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution" is displayed.

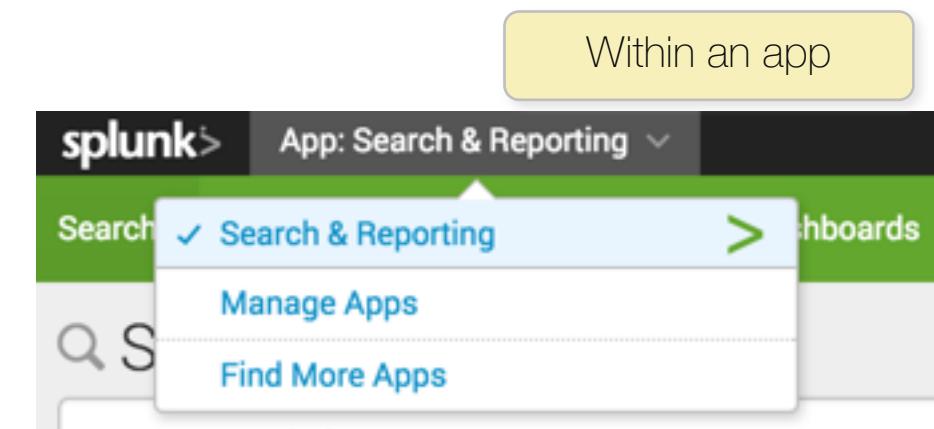
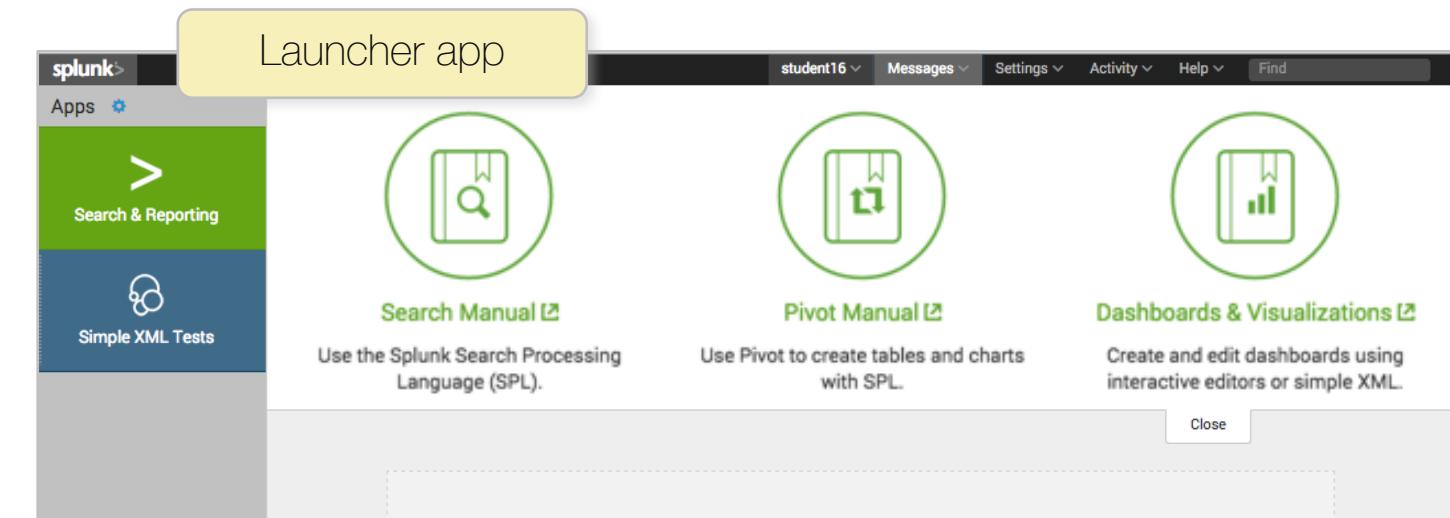
Users and Roles

- 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
- The account you use for the lab exercises has the **power** role



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 create or install additional apps to your Splunk instance from
<http://splunkbase.splunk.com>



Note

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

Home App

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



The screenshot shows the Splunk Home App interface. At the top, there's a navigation bar with 'student16' and various dropdown menus like 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the navigation is a 'splunk>' logo. A green box highlights the 'Search & Reporting' button under the 'Apps' section. A yellow callout box labeled 'Select app context' points to this button. To the right, there's a section titled 'Explore Splunk Enterprise' with three circular icons: 'Search Manual' (book with magnifying glass), 'Pivot Manual' (book with table), and 'Dashboards & Visualizations' (book with chart). A yellow callout box labeled 'Links to several helpful resources' points to these manuals. At the bottom, there's a dashed-line box containing six small dashboard icons (bar charts, line graphs, etc.) with the text 'Choose a home dashboard'. A yellow callout box labeled 'After you've built dashboards with your data, you can choose one to appear in your Launcher app' points to this area.

Explore Splunk Enterprise

student16 Messages Settings Activity Help Find

Apps >

Search & Reporting

Select app context

Search Manual

Pivot Manual

Dashboards & Visualizations

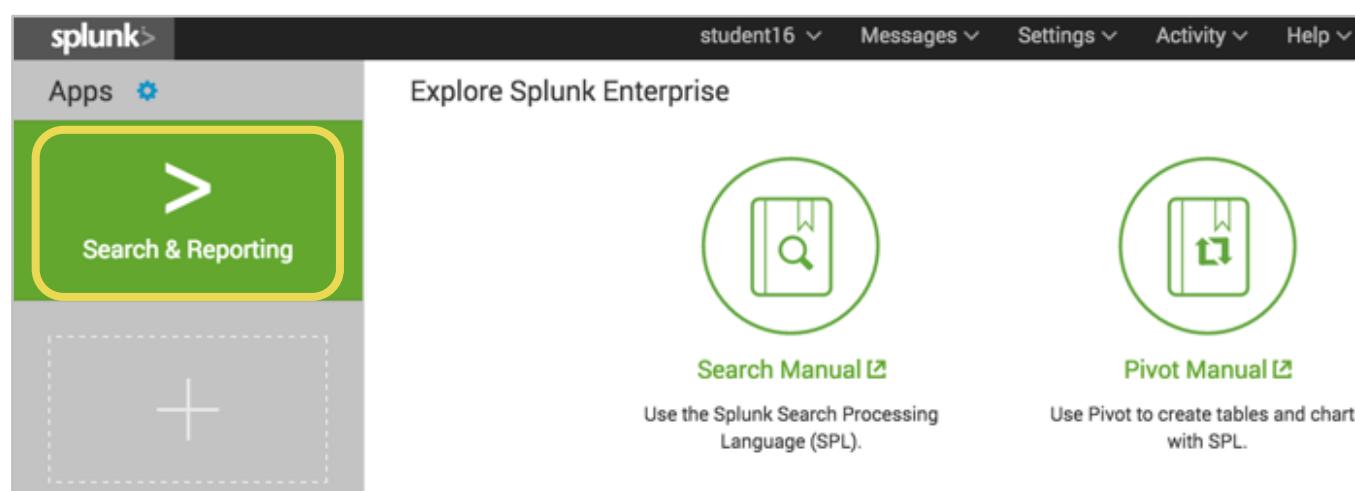
Close

Choose a home dashboard

Generated for Anil Gogia (6756585) (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**



This screenshot shows the 'Search & Reporting' app view. At the top, the navigation bar has 'splunk>' and 'App: Search & Reporting'. The 'Search & Reporting' link in the dropdown menu is highlighted with a yellow box. Below the navigation is a search bar with 'enter search here...' and a dropdown menu for 'No Event Sampling'. To the right, there are sections titled 'How to Search' and 'What to Search', both containing descriptive text and statistics: '2,010,356 Events INDEXED'.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module 4: Inputs

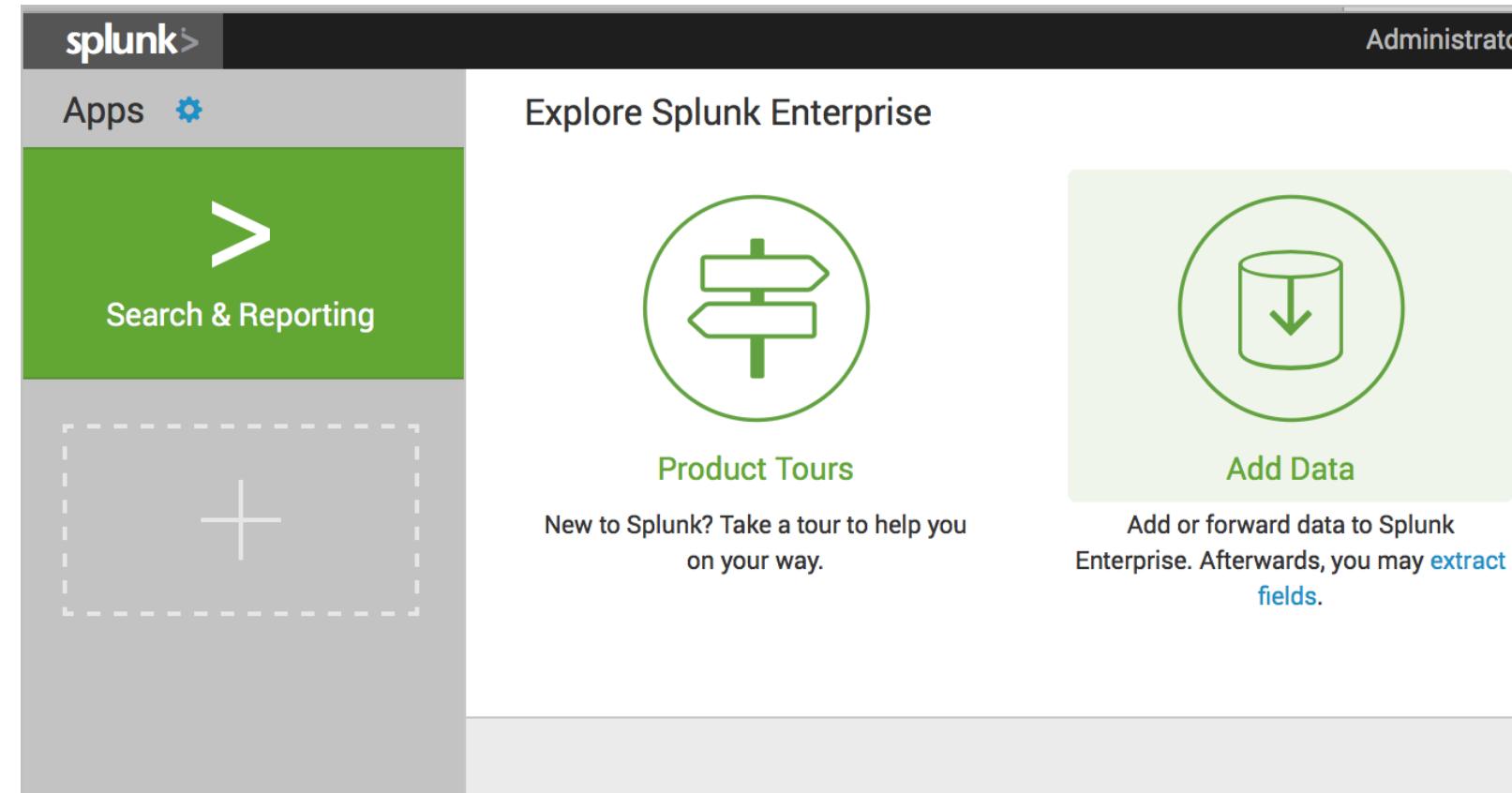
Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module Objectives

- Identify the input types
- Uploading data using Splunk Web
- Using the Monitor option

Adding Data

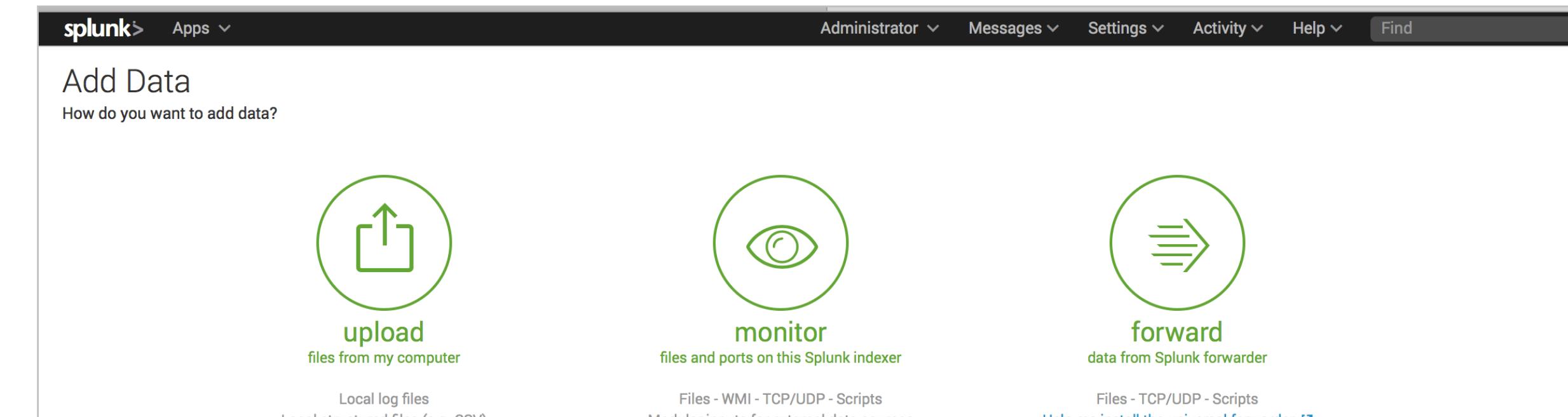
Administrators can access the Add Data menu by clicking the Add Data icon located on the Splunk Enterprise home app



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Add Data Menu

Add Data menu provides three options depending on the source to be used



Upload Option

Upload option allows users to upload local files that only get indexed once. Useful for testing or data that is created once and never gets updated.

Monitor Option

Monitors files, directories, http events, network ports, or data gathering scripts located on Splunk Enterprise instances.

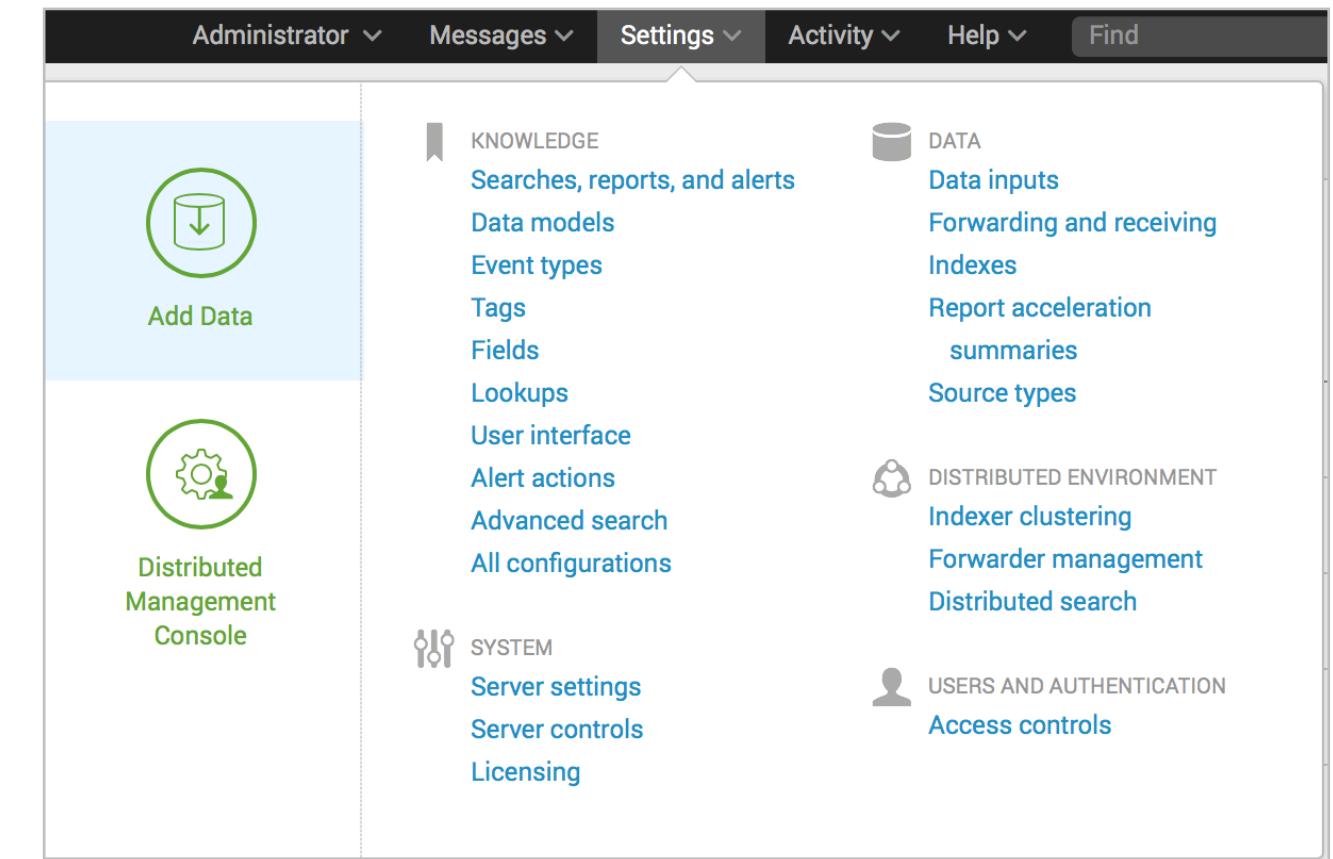
Forward Option

Main source of input in most production environments. Installed on remote machines where data is gathered on forwarded to an index over a receiving port.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Additional Data Input Management Options

- Data can also be added and managed by:
 - **Settings > Data** Inputs below the **Data** header
 - Splunk CLI
 - Editing .conf files



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Using the Upload Option

Ideal for testing and searching small datasets that are not updated

The screenshot shows the Splunk interface with the following steps:

- Step 1:** Click the **Upload icon** (highlighted with a yellow box and orange circle).
- Step 2:** Two options to upload a local dataset:
 - Click the **Select File** button and choose a local file, or
 - Drag and drop the file
- Step 3:** Click **Next >** (highlighted with a yellow box and orange circle).

Key UI elements include:

- Splunk logo and navigation bar: Apps, Administrator, Messages, Settings, Activity, Help, Find.
- Progress bar: Select Source (green dot), Set Source Type, Input Settings, Review, Done.
- Buttons: Select File, Next >, Done.
- Text: "Select Source", "Choose a file to upload to Splunk, either by browsing your computer or by dropping a file into the target box below.", "Selected File: CustomerSurvey.csv", "Drop your data file here", "The maximum file upload size is 500 Mb".
- Links: "Learn More", "Tutorial for adding data".

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Set Sourcetype

The screenshot shows the Splunk 'Add Data' interface. The top navigation bar includes 'splunk> Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the navigation is a progress bar with steps: 'Add Data' (green dot), 'Select Source' (grey dot), 'Set Source Type' (green dot, currently selected), 'Input Settings' (grey dot), 'Review' (grey dot), and 'Done' (grey dot). A 'Next >' button is located next to the 'Review' step. A yellow callout box points to the 'Next >' button with the text: 'If the data separation format is acceptable, click Next'.

Set Source Type

This page lets you see how Splunk sees your data. Use the options below to define proper event breaks and time fields.

Source: CustomerSurvey.csv

Data recognized by Splunk will be assigned a pre-trained sourcetype (e.g. CSV file)

Save As

Table Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 9 ... Next >

	_time	AccountId	age	bday	city	CONTENT_QUALITY	CONTE
1	10/13/15	61181	40	1975-07-20 00:00:00	Norlane	5	5
3	10/13/15 8:58:42.000 PM	22892	19	1996-07-13 00:00:00	Marmora	5	3
4	10/13/15 8:47:36.000 PM	103339	43	1972-10-18 00:00:00	Cividate Camuno	1	5

Using the **Source type** drop down menu, you can change the data to a different predefined source type or create a new one.

Source type: csv

filter

- > Default Settings
- > Application
- > Database
- > Email
- > Miscellaneous
- > Network & Security
- > Operating System
- > Structured
- > Uncategorized
- > Web

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Adjusting Time Stamps and Event Breaks

splunk > Apps > Add Data > Set Source Type > Input Settings > Review > Done

Set Source Type

This page lets you see how Splunk sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: CustomerSurvey.csv

Source type: csv Save As

Timestamp

Extraction Auto Current time Advanced...

Delimited settings

Field delimiter (comma) ▼

Quote character (double quote) " ▼

File preamble

A regular expression that instructs Splunk to ignore these preamble lines within the file.

Field names Auto Line... Custom... Regex...

	_time	AccountId	age	bday	city	CO
1	10/13/15 10:14:00.000 PM	61181	40	1975-07- 20 00:00:00	Norlane	5
2	10/13/15 9:29:28.000 PM	26554	44	1971-08- 11 00:00:00	Marmora	5
3	10/13/15 8:58:42.000 PM	22892	19	1996-07- 13 00:00:00	Sycamore	4
4	10/13/15 8:47:36.000 PM	103339	43	1972-10- 18 00:00:00	Cividate Camuno	1

Note



The menus will change depending on the sourcetype selected.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

How Splunk Uses Sourcetypes with Data

- **sourcetype** is Splunk's way of categorizing the type of data
 - Splunk indexing processes frequently reference sourcetype
 - Many searches, reports, dashboards, apps, etc. also rely on sourcetype
 - When using predefined sourcetypes, Splunk knows where to break the event, the location of the timestamp, and automatically create field value pairs.

Splunk Data View										
Table		Format		20 Per Page						
	_time	AccountId	age	bday	city	CONTENT_QUALITY	CONTENT_QUANTITY	country	DESIGN	email
1	10/13/15 9:29:28.000 PM	26554	44	1971-08- 11 00:00:00	Marmora	5	3	US	4	uabbott@yahoo.com
2	10/13/15 8:09:05.000 PM	55084	43	1972-04- 09 00:00:00	Tarko-Sale	3	3	RU	4	kernser@gmail.com

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

How Splunk Uses Sourcetypes with Data (cont.)

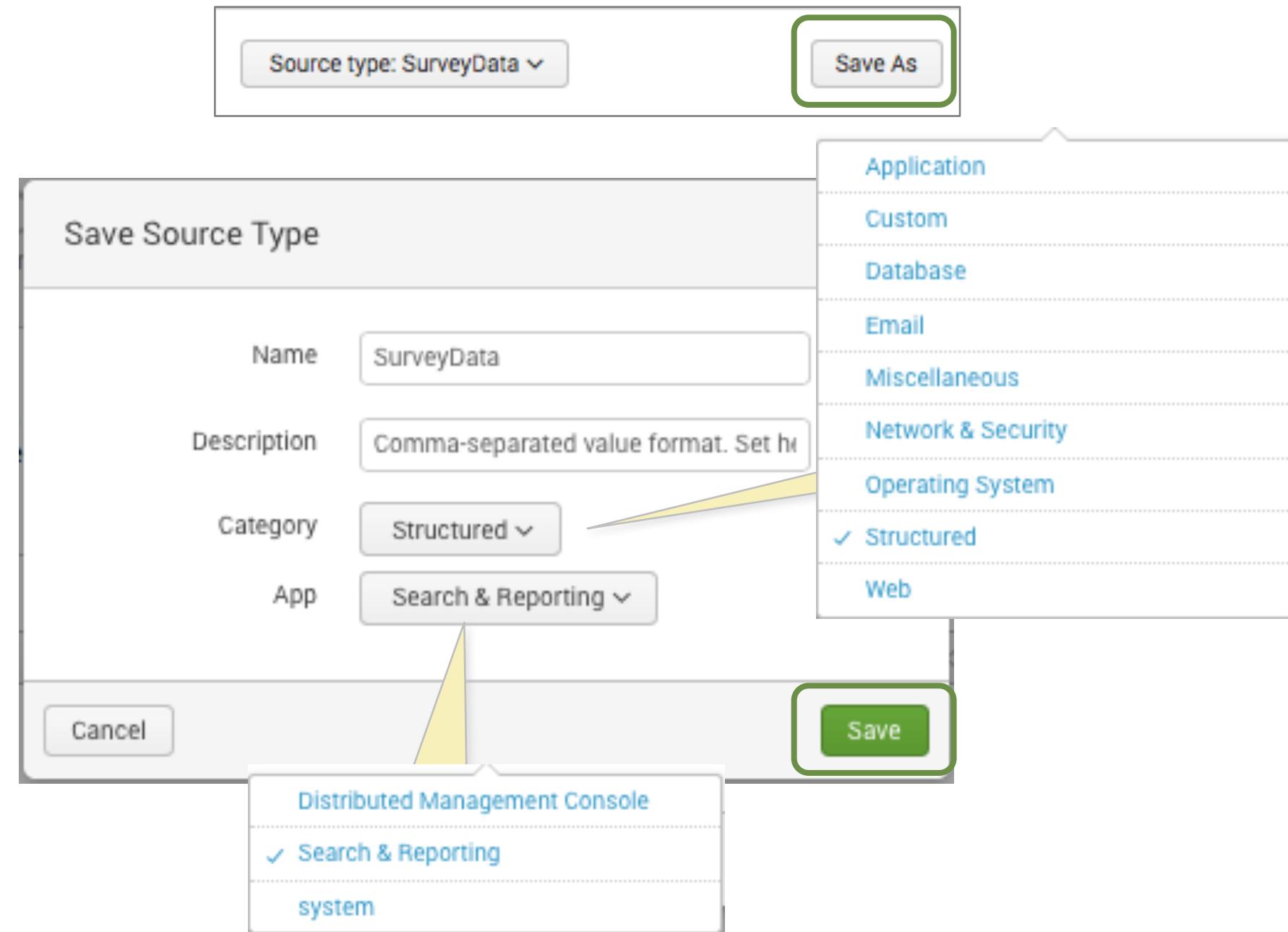
- When Splunk does not have a predefined way to break events, it looks for a time stamp to break the data
 - In the case of multiple time stamps, a regular expression can be used to extract the desired time
 - Regular expressions can be used with any expected patterns in the data to create a line break

	Time	Event
1	⚠ 6/3/16 12:38:47.000 PM	AccountId,"CONTENT_QUALITY","CONTENT_QUANTITY",DESIGN,JSESSIONID,NAVIGATION,SATISFACTION,"_raw","_time",age,bday,"change_type",city,country,"date_hour","date_mday","date_minute","date_month","date_second","date_wday","date_year","date_zone",email,eventtype,fname,gender,host,index,karma,lat,linecount,lname,lon,punct,region,registered,"site_release",source,sourcetype,"splunk_server","splunk_server_group",tag,"tag::eventtype",timeendpos,timestartpos,username timestamp = none
2	10/13/15 10:14:00.000 PM	61181,5,5,4,SD9SL6FF5ADFF2948092910,3,4,"[13/Oct/2015:22:14:00] AccountId=61181 JSESSIONID=SD9SL6FF5ADFF2948092910 site_release=v4.1
3	10/13/15 5:14:00.000 PM	CONTENT_QUANTITY=5 CONTENT_QUALITY=5 NAVIGATION=3 DESIGN=4 SATISFACTION=4", "2015-10-13T15:14:00.000-0700", 40, "1975-07-20 00:00:00",,Norlane,AU,22,13,14,october,0,tuesday,2015,local,"jauer@kuvalis.org", "nix-all-logs",Arno,M,"customer_survey",,main,6807,"-38.1014",2,Mante,"144.3542", "[//::::]_==_.=t=t=t=t=",Victoria,"2009-01-26 00:00:00", "v4.1", "/opt/log/customer_survey/bcg_survey.log", "bcg_survey-3", "ip-10-222-134-157",,,21,1,mhammes

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Saving Sourcetypes

- You have the following options to save sourcetypes if any changes were made
 - Name
 - Description
 - Select a category to store in the predefined menu
 - Select which app context to save it to



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Input Settings

The screenshot shows the 'Add Data' wizard in the 'Input Settings' step. The navigation bar includes 'Select Source', 'Set Source Type', 'Input Settings' (highlighted in green), 'Review', and 'Done'. A green progress bar indicates the current step.

Input Settings
Optional set additional input parameters for this data input as follows:

Host
When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

The 'Host field value' is set to 'splunkServer1'. A yellow callout box states: "The host name should reflect the machine the events are originating from."

Index
Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

The 'Index' dropdown is set to 'surveydata'. A yellow callout box states: "Select the index to import the data. You can also create a new one if needed."

FAQ

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Review and Submit

Add Data

Select Source Set Source Type Input Settings Review Done **Submit >**

Review

Input Type	Uploaded File
File Name	CustomerSurvey.csv
Source Type	SurveyData
Host	splunkServer1
Index	surveydata

The Review page displays the settings for our input.

Add Data

Select Source Set Source Type Input Settings **Review** **Done**

File input has been created successfully.

Configure your inputs by going to [Settings > Data Inputs](#)

Start Searching Search your data now or see [examples and tutorials](#).

Extract Fields Create search-time field extractions. [Learn more about fields](#).

Add More Data Add more data inputs now or see [examples and tutorials](#).

Download Apps Apps help you do more with your data. [Learn more](#).

Build Dashboards Visualize your searches. [Learn more](#).

After clicking **Submit**, Splunk indexes the data, and we can start searching

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Using the Monitor Option

Monitors files, directories, http events, network ports, or data gathering scripts located on a Splunk indexer

The screenshot shows the Splunk UI with the following annotations:

- Step 1:** A callout points to the "Monitor" icon in the top-left corner of the main content area. The icon is a green eye inside a circle. The text "Click the Monitor icon" is inside the callout.
- Step 2:** A callout points to the "Files & Directories" section in the "Add Data" wizard. The text "Options to monitor files, directories, http events, ports, or monitor sources with custom script you can write." is inside the callout, with a green bracket pointing from the "option" text to the "Files & Directories" section.

splunk> Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾

Add Data Select Source Input Settings Review Done < Next >

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure Splunk to listen on a network port.

Scripts
Get data from from any API, service, or database with a script.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Monitoring Files or Directories

The screenshot shows the Splunk interface for adding data. The top navigation bar includes 'splunk> Apps < Find' and dropdowns for 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below the navigation is a progress bar with steps: 'Add Data' (green dot), 'Select Source' (green dot), 'Set Source Type' (grey dot), 'Input Settings' (grey dot), 'Review' (grey dot), and 'Done' (empty circle). A 'Next >' button is on the right.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure Splunk to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Select Source (highlighted)

Set Source Type

Input Settings

Review

Done

Next >

Browse to select the file or directory. (yellow callout pointing to the 'File or Directory' input field)

File or Directory? (link to help)

/opt/log/www1/access.log

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Select the option to continuously monitor or index the data once. (yellow callout pointing to the 'Continuously Monitor' and 'Index Once' buttons)

Continuously Monitor

Whitelist?

Blacklist?

When a directory is selected, there are options to whitelist or blacklist files in the directory. (yellow callout pointing to the 'Whitelist?' and 'Blacklist?' fields)

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Monitoring Files or Directories (cont)

The screenshot shows the Splunk 'Add Data' interface in the 'Input Settings' step. The top navigation bar includes 'splunk> Apps <' and 'Administrator > Messages <'. The main title is 'Add Data' with a progress bar at the top. The steps are: Select Source (green), Set Source Type (green), Input Settings (yellow), Review (grey), and Done (grey). The 'Review' button is highlighted in green.

Input Settings
Optionaly set additional input parameters for this data input as follows:

App context
Application contexts are folders within a Splunk instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. [Learn More ↗](#)

Host
When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input options. [Learn More ↗](#)

Index
Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More ↗](#)

Browse to select the file or directory.

Host field value

Index main ▾ Create a new index

Constant value Regular expression on path Segment in path
ip-10-61-154-123

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Using the Forward Option

- Production environments use forwarders as the main source of data input
 - Installed on remote machines and forward data to an indexer over a receiving

The screenshot shows the Splunk Add Data interface. At the top, there's a navigation bar with the Splunk logo and an Apps dropdown. Below it, a progress bar indicates the current step: "Select Forwarders" (green), followed by "Select Source" (grey), "Input Settings" (grey), and "Review & Save" (grey). To the right of the progress bar are "Back" and "Next >" buttons. A green callout box labeled "Note" contains the text: "Only forwarders setup to use the server will be displayed in this interface, regardless of sending data to the server." At the bottom, a warning message in a red-bordered box states: "There are currently no forwarders configured as deployment clients to this instance. [Learn More](#)". On the left side of the main content area, there's a sidebar with a "forward" icon and the text "data from Splunk forwarder". Below the sidebar, there are links for "Files - TCP/UDP - Scripts" and a link to "Help me install the universal forwarder".

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

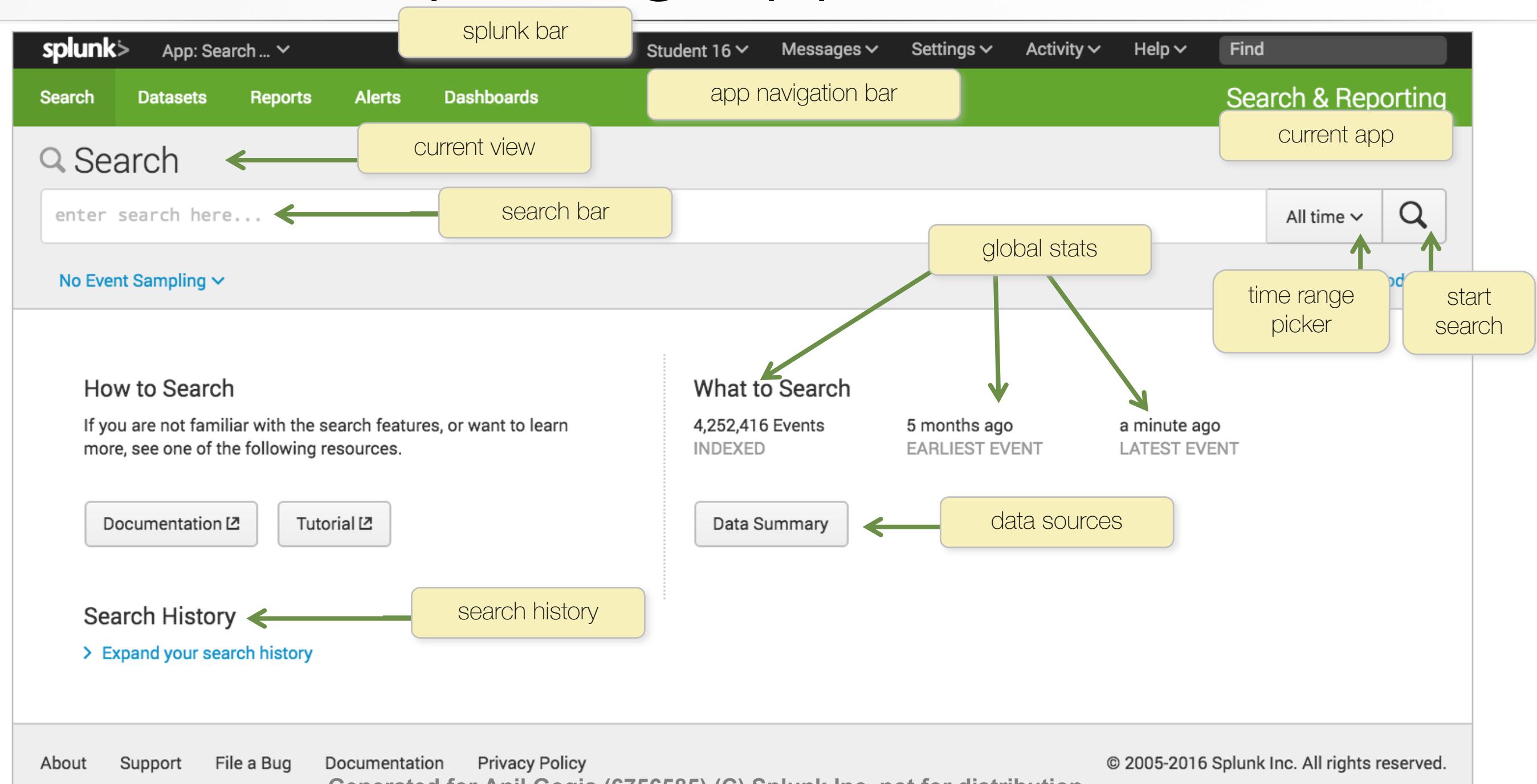
Module 5: Searching

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module Objectives

- Run basic searches
- Use autocomplete to help build a search
- Set the time range of a search
- Identify the contents of search results
- Refine searches
- Use the timeline
- Control a search job
- Save search results

Search & Reporting App Overview (cont.)



Data Summary Tabs

The screenshot shows the Splunk web interface. At the top, there's a navigation bar with links for Search, Datasets, Reports, Alerts, Dashboards, Student 16, Messages, Settings, Activity, Help, and Find. Below the navigation bar is a search bar with a placeholder 'enter search here...' and a date range selector set to 'Yesterday'. A yellow callout box on the right says 'Click **Data Summary** to see hosts, sources, or sourcetypes on separate tabs'. In the main content area, there are three tabs labeled 'Data Summary': 'Hosts (10)', 'Sources (27)', and 'Sourcetypes (11)'. The 'Hosts' tab is currently selected. On the left, there's a sidebar with sections for 'How to Search' and 'What to Search'. The 'What to Search' section displays '4,284,524 Events INDEXED' and '5 months ago EARLIEST EVENT'. A green arrow points from the 'Data Summary' button in the sidebar to the 'Hosts (10)' tab. Another green arrow points from the 'Hosts (10)' tab to the list of hosts on the right. A third green arrow points from the 'Sourcetypes (11)' tab to the list of sourcetypes on the far right. A yellow callout box on the right side of the sourcetype list says 'Tables can be sorted or filtered'. The host list contains entries like 'adldapsv1', 'badgesv1', 'cisco_router1', etc. The sourcetype list contains entries like 'access_combined', 'cisco_esa', 'cisco_firewall', etc.

- **Host** – Host name, 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

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Key Details

The screenshot shows the Splunk Search & Reporting interface. The search bar contains the query "error OR fail*". The results section shows 6,382 events from October 10, 2016, between 12:00:00.000 AM and 12:00:00.000 AM. A timeline visualization highlights a cluster of 255 events at 10 PM on Monday, October 10, 2016. The event list table includes columns for Time, Event, host, source, and sourcetype. A note box provides information about Splunk's glossary and Splexicon.

error OR fail*

search

6,382 events (10/10/16 12:00:00.000 AM to 10/11/16 12:00:00.000 AM) No Event Sampling

Events (6,382) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection × Deselect 1 hour per column

255 events at 10 PM on Monday, October 10, 2016

List Format 20 Per Page

< Prev 1 2 3 4 5 6 7 8 9 ... Next >

i	Time	Event
>	10/10/16 11:59:54.000 PM	Mon Oct 10 2016 23:59:54 www2 sshd[3286]: Failed password for nsharpe from 10.2.10.163 port 447 2 ssh2 host = www2 source = /opt/log/www2/secure.log sourcetype = linux_secure
>	10/10/16 11:59:47.000 PM	Mon Oct 10 2016 23:59:47 www3 sshd[5941]: Failed password for invalid user brian from 223.205.2 19.67 port 2483 ssh2 host = www3 source = /opt/log/www3/secure.log sourcetype = linux_secure
>	10/10/16 11:59:30.000 PM	Mon Oct 10 2016 23:59:30 www3 sshd[4837]: Failed password for invalid user .67 port 2103 ssh2 host = www3 source = /opt/log/www3/secure.log sourcetype = linux_secure
>	10/10/16 11:59:22.000 PM	Mon Oct 10 2016 23:59:22 www3 sshd[4733]: Failed password for invalid user 9.67 port 4 host = www3 source = /opt/log/www3/secure.log sourcetype = linux_secure

< Hide Fields All Fields event

Selected Fields a host 6 a source 9 a sourcetype 4

Interesting Fields a action 2 a app 1 # date_hour 24 # date_mday 1 # date_minute 60

Note

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

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Why Learn to Search?

- Why is it important to be able to write searches?
 - You have questions about your data -- searches retrieve the events that can answer them
 - Every report and visualization is built based on an underlying search
 - Understanding, analyzing, and troubleshooting visualizations depends on your ability to understand the search string
 - Mastering the search language enables you to do as much as possible with your data to meet your specific needs

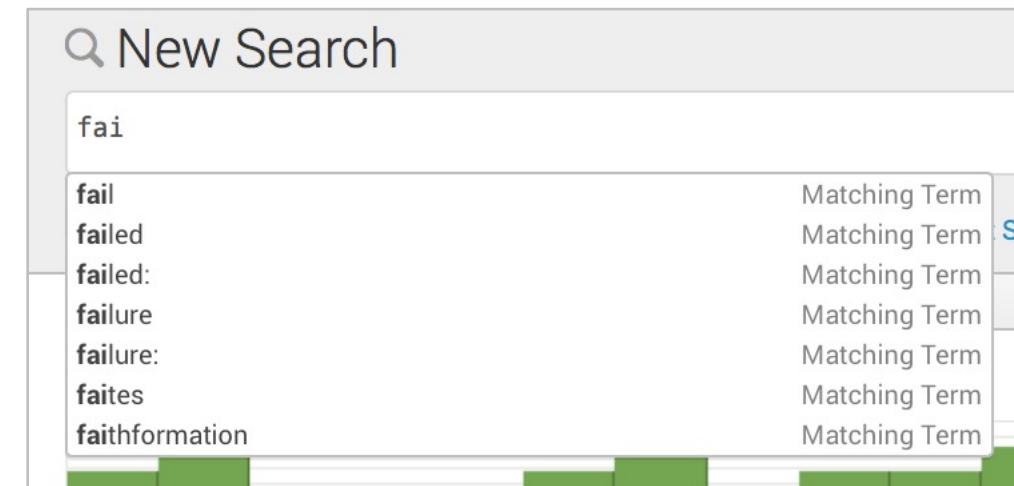
Search Guidelines

- * 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

fail	Yesterday	🔍
fail*	Yesterday	🔍
fail* nfs	Yesterday	🔍
error OR 404	Yesterday	🔍
error OR failed AND 500 OR 503	Yesterday	🔍
error OR (failed AND (500 OR 503))	Yesterday	🔍
"login failure"	Yesterday	🔍

Search Assistant

- Search Assistant provides selections for how to complete the search string
- Before the first pipe (|), it will look for matching terms
- You can continue typing OR select a term from the list
 - If you select a term from the list, it is added to the search



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Search Assistant (cont.)

- After the first pipe, the Search Assistant will show a list of commands that can be entered into the search string
- You can continue typing OR scroll through and select a command to add
- If you mouse over a command, more information about the command is shown
- As you continue to type, Search Assistant makes more suggestions **B**

A screenshot of the Splunk Search Assistant interface. The search bar contains the partial command `failed | cha`. A dropdown menu is open, listing several command suggestions:

- `chart` (highlighted)
- `sichart`
- `timechart`
- `sitimechart`
- `chart` (disabled, with a note: "Returns results in a tabular output for charting.")

The interface also shows a summary: `Events (16)` and a green progress bar indicating the search is in progress.

A screenshot of the Splunk Search Assistant interface. The search bar contains the command `failed | chart cou`. A dropdown menu is open, listing several command suggestions:

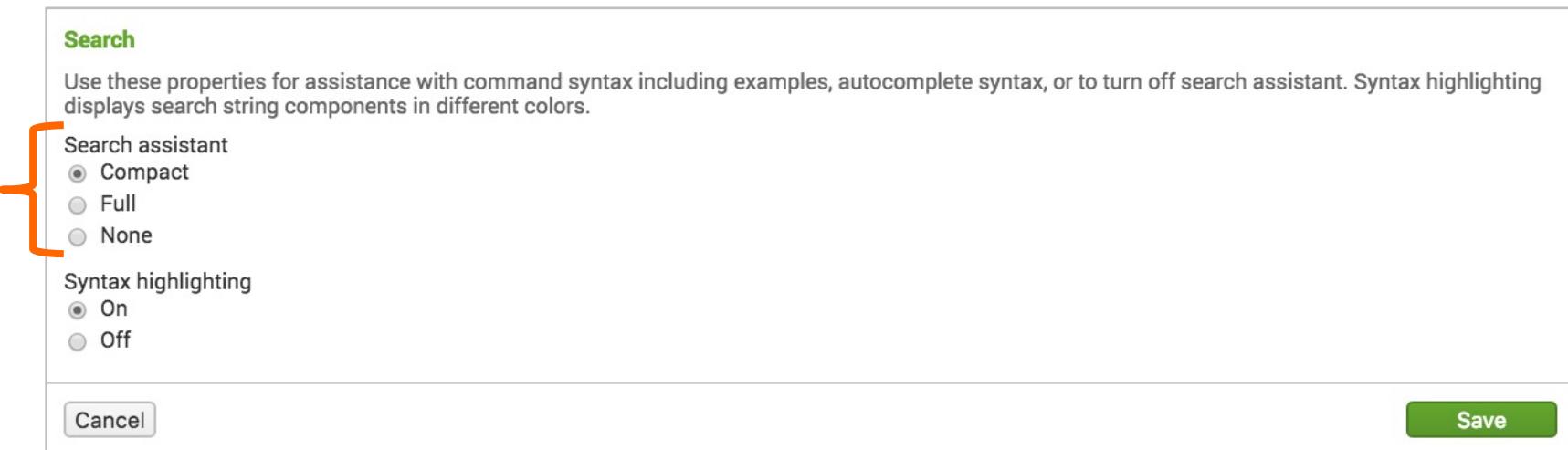
- `count` (highlighted)
- `chart count by host`
- `chart count by src_ip`
- `chart count by user`
- `chart count(_raw) by action`
- `chart count(_raw) by saved_search`
- `chart` (disabled, with a note: "Returns results in a tabular output for charting.")

The interface shows a summary: `Events (16)` and a green progress bar. A tooltip labeled **B** points to the `count` suggestion.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Search Assistant (cont.)

- Search Assistant is enabled by default, in the user settings
- By default, **Compact** is selected
- If desired, to show more information, choose **Full**



Compact

Search

failed | chart cou

No Event Sampling

count
chart count by host
chart count by src_ip
chart count by user
chart count over vendor_action by src_ip
chart count(_raw) by action

How to Search

If you are not finding what you're looking for, try one of these:

chart
Returns results in a tabular output for charting.
Example:
... | chart max(delay) over foo

Command History

Command Args

Learn More ↗

Full

Search

failed | chart cou

Command History

... | chart count by host
... | chart count by user
... | chart count by src_ip
... | chart count over vendor_action by src_ip
... | chart count(_raw) by action

Command Args

count

chart Help More ✓ Auto Open

Returns results in a tabular output for charting.

Examples

Return max(delay) for each value of foo.
... | chart max(delay) over foo

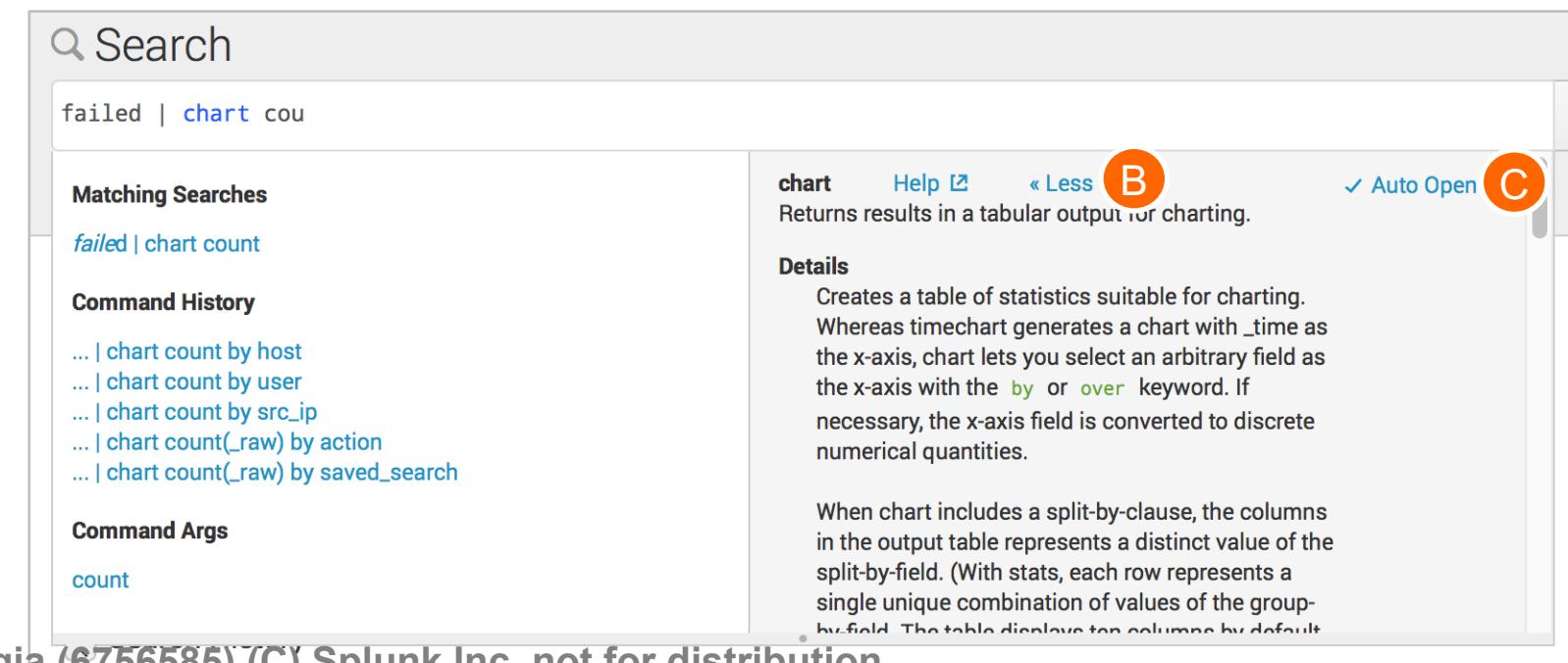
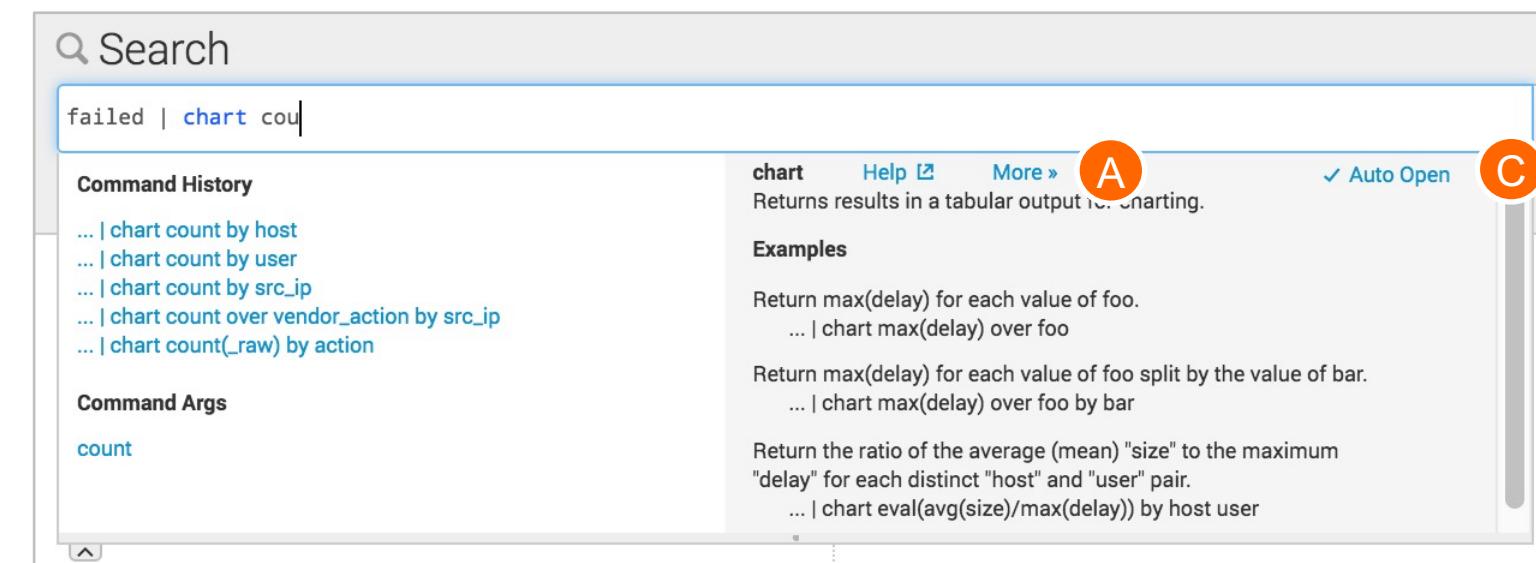
Return max(delay) for each value of foo split by the value of bar.
... | chart max(delay) over foo by bar

Return the ratio of the average (mean) "size" to the maximum "delay" for each distinct "host" and "user" pair.
... | chart eval(avg(size)/max(delay)) by host user

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Search Assistant - Full

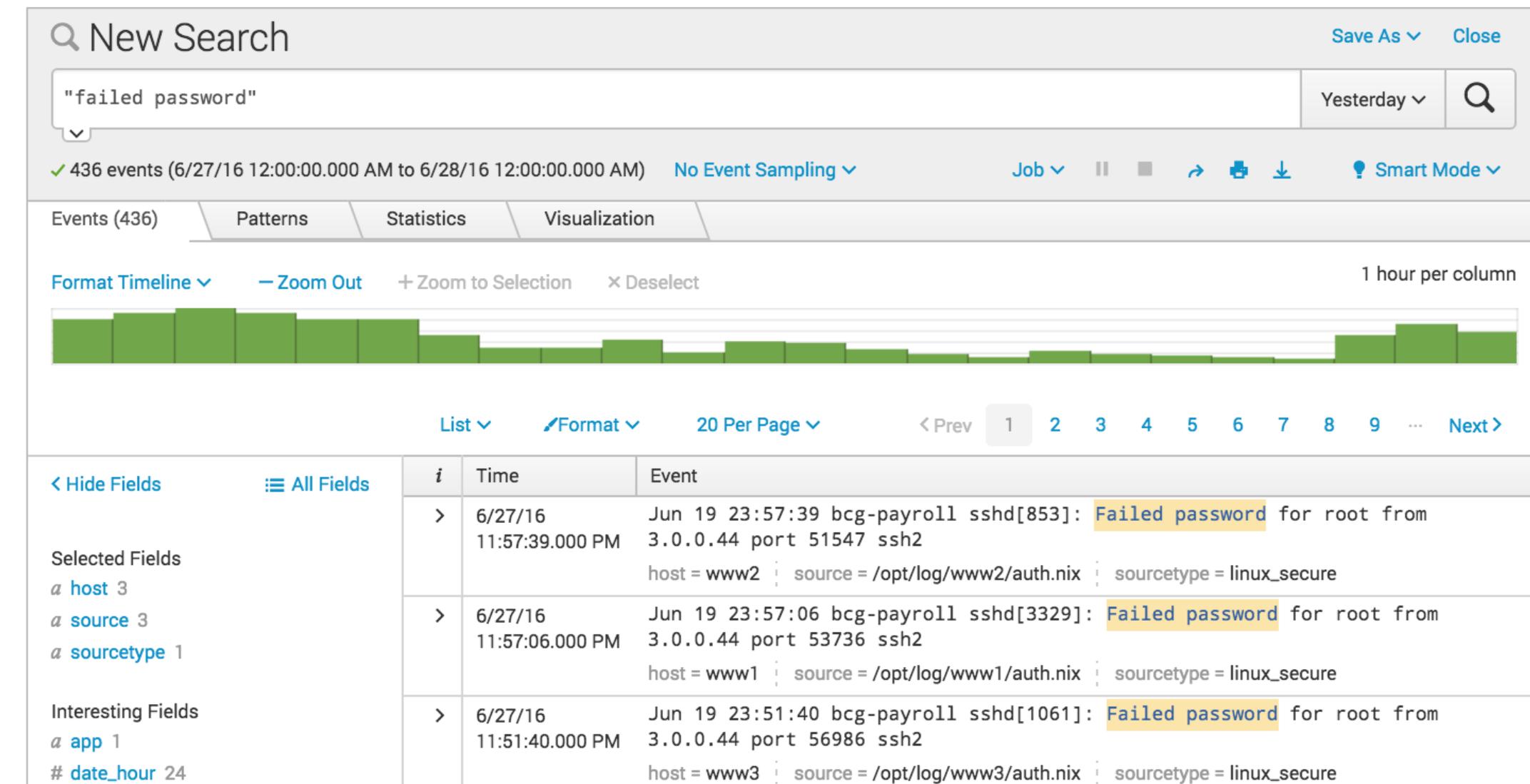
- A To show more information, click **More >**
- B To show less information, click **<< Less**
- C To toggle Full mode off, de-select **Auto Open**



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Search Results

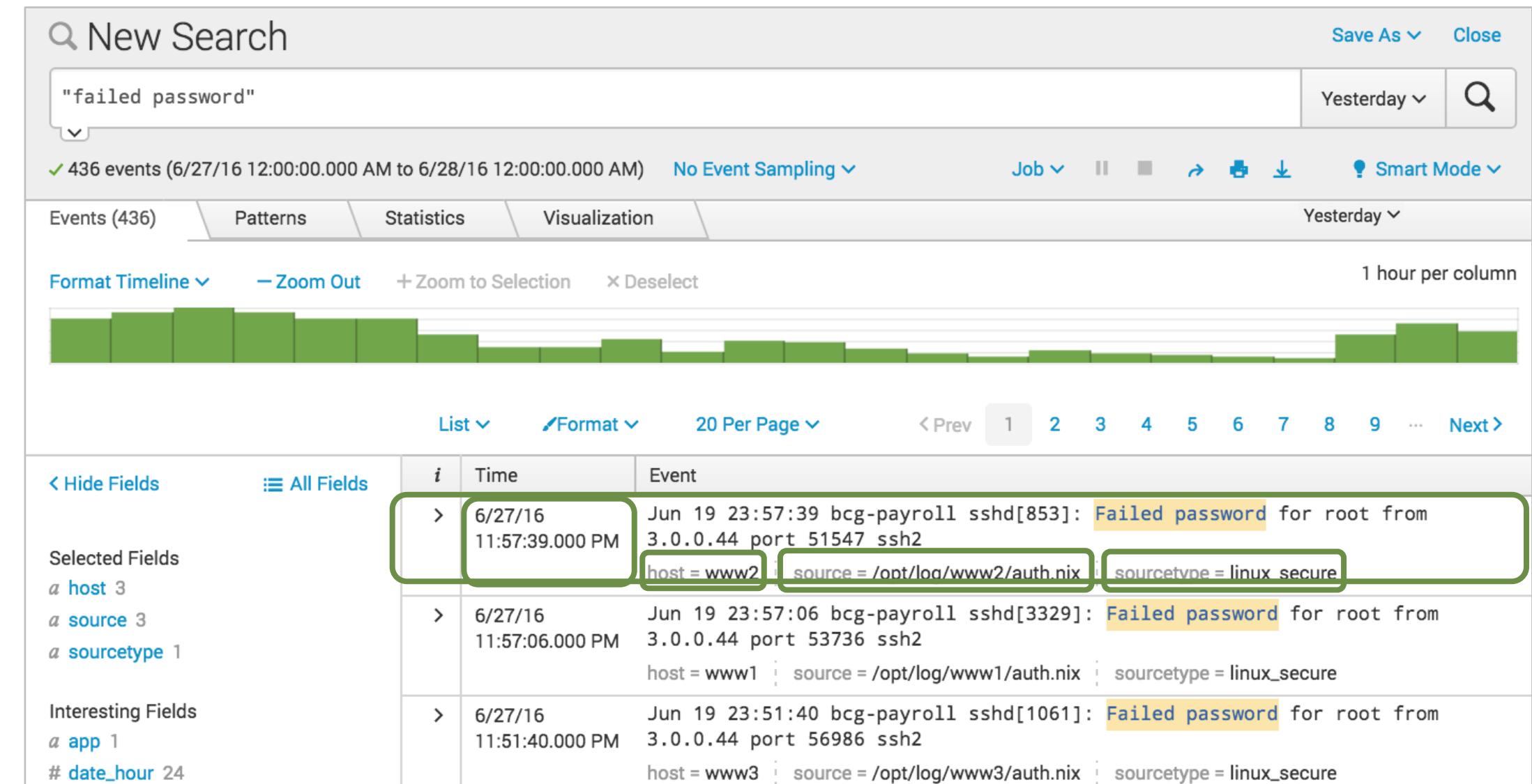
- Matching results are returned immediately
- Displayed in reverse chronological order (newest first)
- Matching search terms are highlighted



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Event Details

- Splunk parses data into individual events
- Each event has a:
 - timestamp
 - host
 - source
 - sourcetype



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Search Results Details

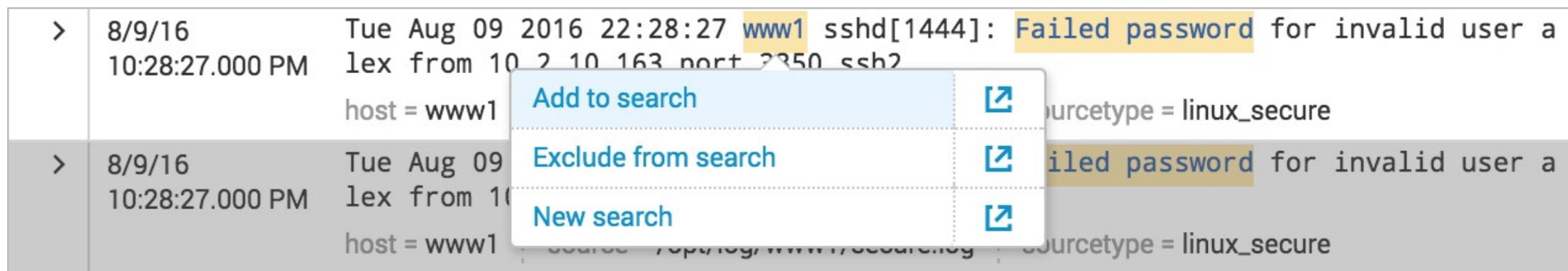
The screenshot shows the Splunk search interface with various UI elements annotated:

- New Search**: The search bar at the top left.
- time range picker**: The time range selector at the top right.
- Save As**: The save button in the top right corner.
- Close**: The close button in the top right corner.
- "failed password"**: The search query in the search bar.
- Events (436)**: The count of events found, with a green arrow pointing to it from the search bar.
- Patterns**, **Statistics**, **Visualization**: Tabs below the search bar.
- No Event Sampling**: The sampling mode setting.
- Job**: The job management dropdown.
- Smart Mode**: The search mode dropdown.
- Events tab**: The tab where search results appear.
- Format Timeline**: The timeline format dropdown.
- timeline**: The timeline visualization below the format dropdown.
- 1 hour per column**: The timeline scale.
- paginator**: The page navigation controls.
- List**, **Format**: The list and format dropdowns.
- 20 Per Page**: The page size dropdown.
- < Prev**, **1**, **2**, **3**, **4**, **5**, **6**, **7**, **8**, **9**, **...**, **Next >**: The page navigation buttons.
- Fields sidebar**: A sidebar on the left containing:
 - < Hide Fields**
 - All Fields**
 - Selected Fields**:
 - host** 3
 - source** 3
 - sourcetype** 1
 - Interesting Fields**:
 - app** 1
 - # date_hour** 24
- events**: A large green bracket on the right side of the table.
- timestamp**: The timestamp field in the table.
- Event**: The event details in the table.
- Jun 19 23:57:39 bcg-payroll sshd[853]: Failed password for root from 3.0.0.4**: An event entry in the table.
- host = www2 | source = /opt/log/www2/auth.nix | sourcetype = linux_secure**: The selected fields for the first event.
- Jun 19 23:57:39 bcg-payroll sshd[3329]: Failed password for root from 3.0.0.4**: Another event entry in the table.
- host = www1 | source = /opt/log/www1/auth.nix | sourcetype = linux_secure**: The selected fields for the second event.
- Jun 19 23:51:40 bcg-payroll sshd[1061]: Failed password for root from 3.0.0.44**: A third event entry in the table.
- host = www3 | source = /opt/log/www3/auth.nix | sourcetype = linux_secure**: The selected fields for the third event.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Using Search Results to Modify a Search

- When you mouse over search results, keywords are highlighted
- Click any item in your search results; a window appears allowing you to:
 - Add the item to the search
 - Exclude the item from the search
 - Open a new search including only that item



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Changing Search Results View Options

You have several layout options for displaying your search results

New Search

"failed password"

Last 7 days

9,208 events (1/13/16 9:00:00.000 PM to 1/20/16 9:10:35.000 PM) No Event Sampling

Events (9,208) Patterns Statistics Visualization

Format Timeline 1 hour per column

List 20 Per Page < Prev 1 2 3 4 5 6 7 8 9 ... Next >

i	Time	Event
>	1/20/16 9:10:31.000 PM	Wed Jan 20 2016 21:10:31 www1 sshd[5283]: Failed password for invalid user desktop from 10.1.10.172 port 1256 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
>	1/20/16 9:10:21.000 PM	Wed Jan 20 2016 21:10:21 www1 sshd[5391]: Failed password for invalid user rdb from 10.1.10.172 port 2469 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
>	1/20/16 9:10:07.000 PM	Wed Jan 20 2016 21:10:07 www1 sshd[1777]: Failed password for invalid user sales from 10.1.10.172 port 2732 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
>	1/20/16 9:09:35.000 PM	Wed Jan 20 2016 21:09:35 www1 sshd[1771]: Failed password for myuan from 10.1.10.172 port 1854 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure

< Hide Fields Selected Fields a host 4 a source 4 a sourcetype 1 Interesting Fields a index 1 # linecount 1 a splunk_server 1 Extract New Fields

Table 20 Per Page < Prev 1 2 3 4 5 6 7

i	_time	host	source	sourcetype
>	1/20/16 9:10:31.000 PM	www1	/opt/log/www1/secure.log	linux_secure
>	1/20/16 9:10:21.000 PM	www1	/opt/log/www1/secure.log	linux_secure
>	1/20/16 9:10:07.000 PM	www1	/opt/log/www1/secure.log	linux_secure

Raw 20 Per Page < Prev 1 2 3 4 5 6 7 8 9 ... Next >

Raw

List

Table

2016 21:10:31 www1 sshd[5283]: Failed password for invalid user desktop from 10.1.10.172 ssh2
2016 21:10:21 www1 sshd[5391]: Failed password for invalid user rdb from 10.1.10.172 port 2469 ssh2
> Wed Jan 20 2016 21:10:07 www1 sshd[1777]: Failed password for invalid user sales from 10.1.10.172 port 2732 ssh2

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Selecting a Specific Time

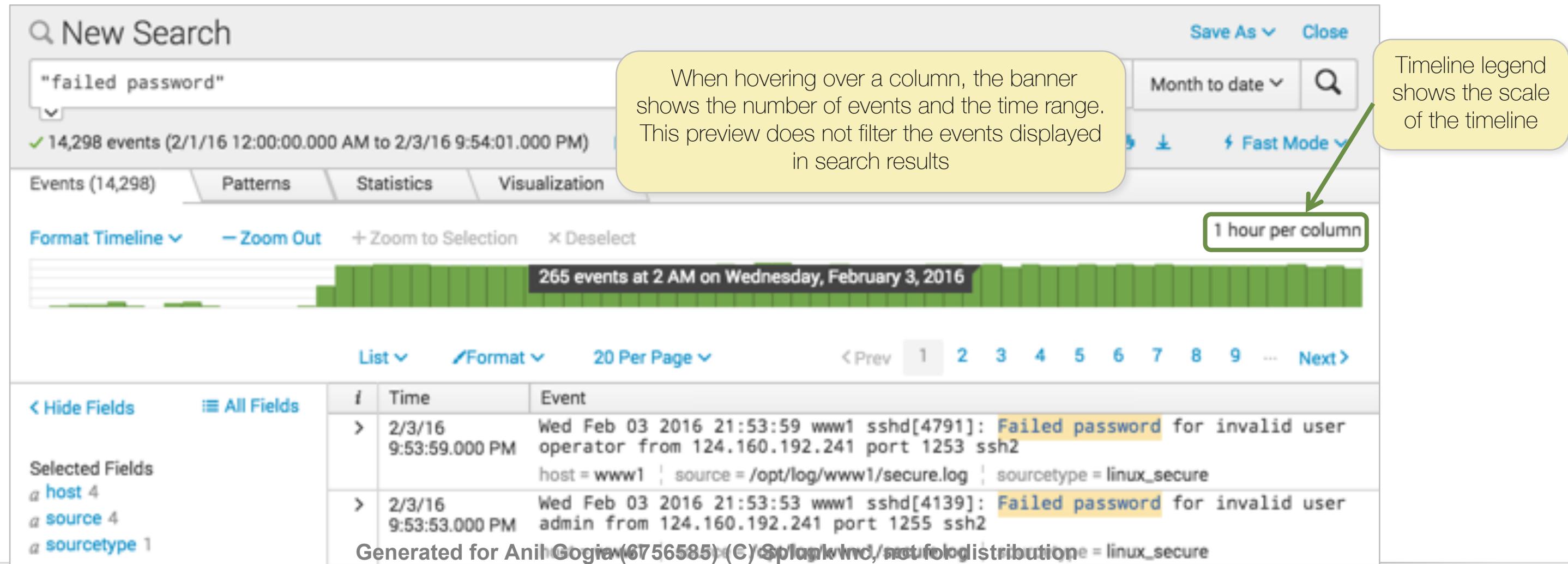
The screenshot shows the Splunk search interface with various time selection methods:

- Relative:** Set Earliest to 7 Days Ago and Latest to now. Options include No Snap-to and Beginning of day.
- Real-time:** Set Earliest to 7 Days Ago and Latest to now. Options include Days Ago and Apply.
- Date Range:** Set Between 01/13/2016 and 01/20/2016, from 00:00:00 to 24:00:00. Options include Between, Apply, and a dropdown for time units.
- Date & Time Range:** Set Between 01/17/2016 at 00:00:00.000 and 01/20/2016 at 21:28:09.000. Options include Between, HH:MM:SS.SSS, and Apply.
- Advanced:** Set Earliest to 1/1/70 12:00:00.000 AM and Latest to 1/20/16 8:58:07.000 PM. Options include Apply and Documentation [!].
- Presets:** A dropdown menu showing various time ranges:
 - 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 business week, Previous month, Previous year
 - Last 15 minutes, Last 60 minutes, Last 4 hours, Last 24 hours, Last 7 days, Last 30 days
 - Other: All timeA yellow callout box labeled "preset time ranges" points to the Presets section.
- Custom Time Ranges:** A green callout box labeled "custom time ranges" points to a list of time range types:
 - > Relative
 - > Real-time
 - > Date Range
 - > Date & Time Range
 - > AdvancedA yellow callout box labeled "custom time ranges" points to this list.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

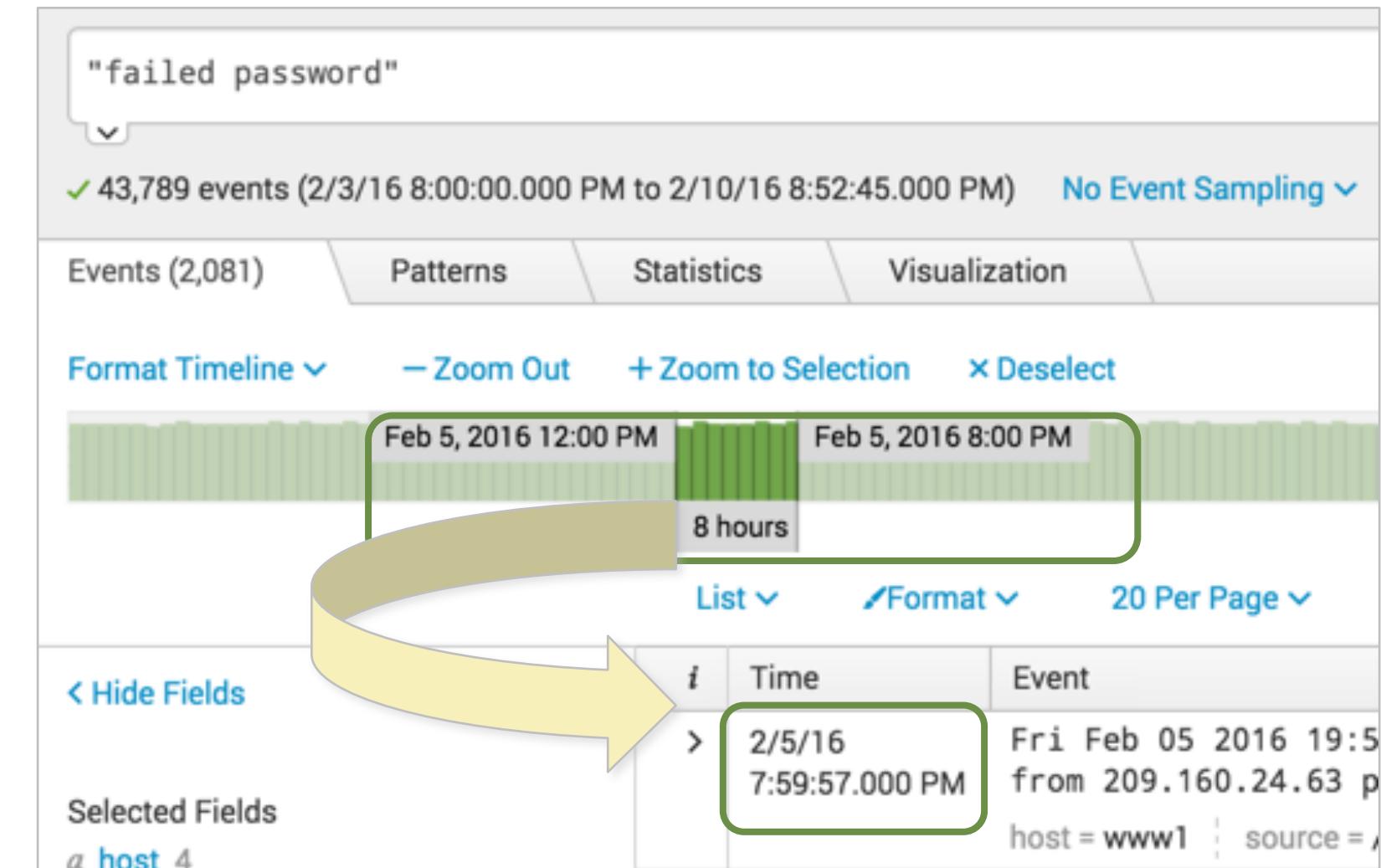
Viewing the Timeline

- Timeline shows distribution of events specified in the time range
 - Mouse over for details, or single-click to filter results for that time period



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-execute the search
 - This filters the events and displays them in reverse chronological order (most recent first)



Use Other Timeline Controls

- **Format Timeline**

- Hides or shows the timeline in different views

- **Zoom Out**

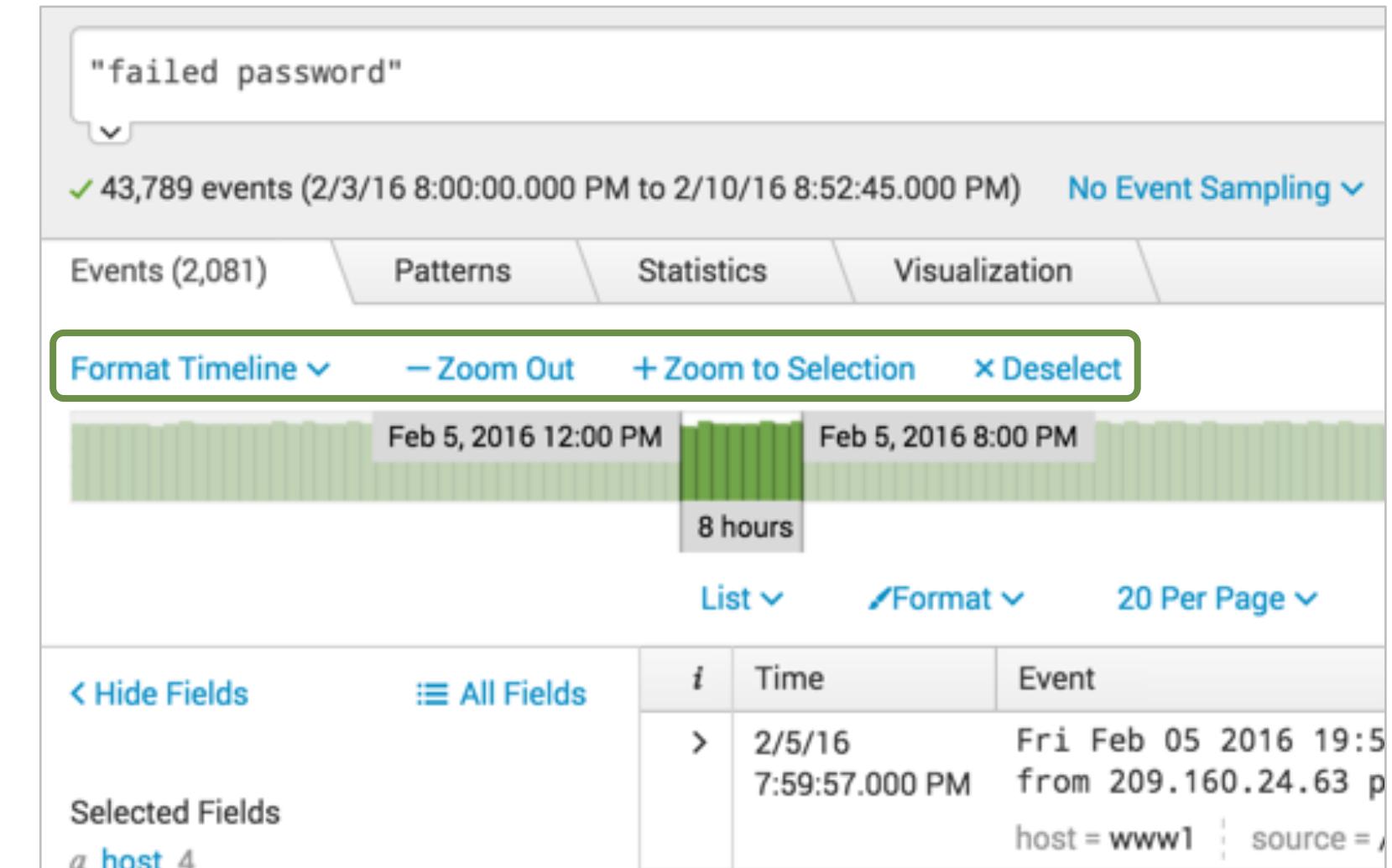
- Expands the time focus and re-executes the search

- **Zoom to Selection**

- Narrows the time range and re-executes the search

- **Deselect**

- If in a drilldown, returns to the original results set
 - Otherwise, grayed out / unavailable

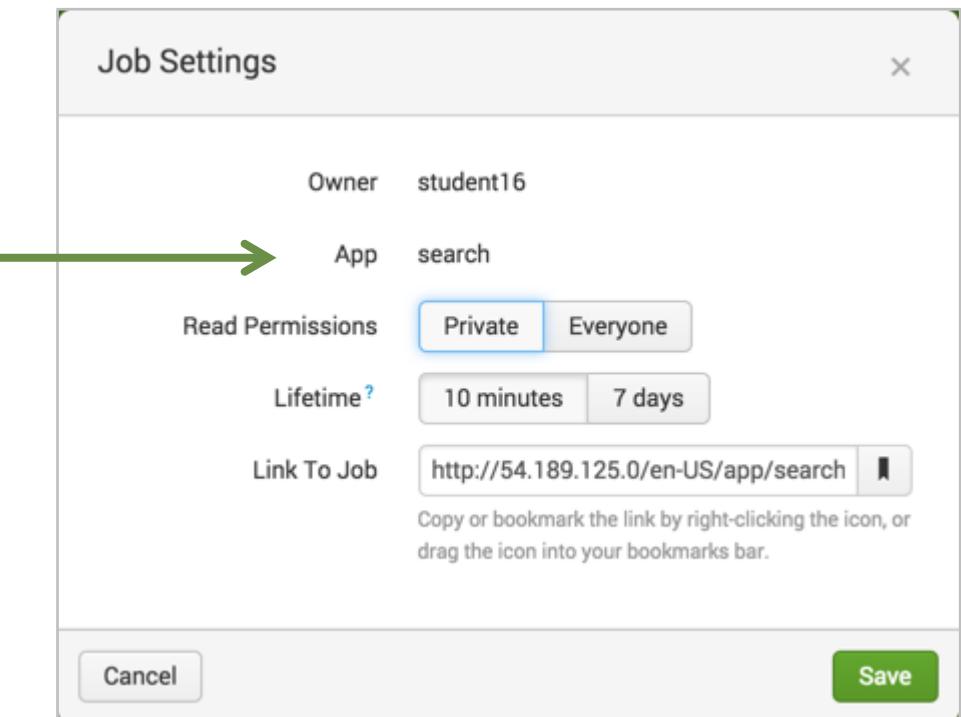


Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Control or Save Search Jobs

- Every search is also a **job**
- Use the Job bar to control search execution
 - **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

The screenshot shows the Splunk search interface with a search bar containing "failed password". Below the search bar, there are tabs for Events (684), Patterns, Statistics, and Visualization. The Job bar at the top right has several icons: a magnifying glass, a pause button, a stop button, a refresh button, a download icon, and a fast mode toggle. A green box highlights the Job dropdown menu, which is open to show options: Edit Job Settings, Send Job to Background, Inspect Job, and Delete Job. The text "Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution" is at the bottom.



Set Permissions

- **Private** [default]

- Only the creator can access

- **Everyone**

- All app users can access search results

- **Lifetime**

- Default is 10 minutes
 - Can be extended to 7 days
 - To keep your search results longer, schedule a report

Job Settings X

Owner becky

App search

Read Permissions Private Everyone

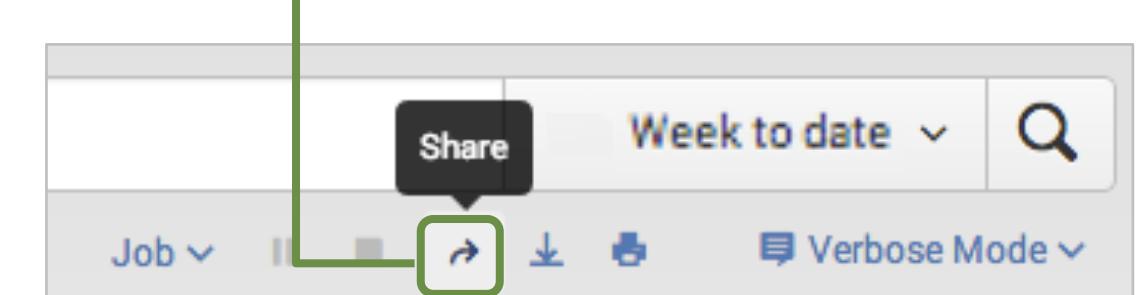
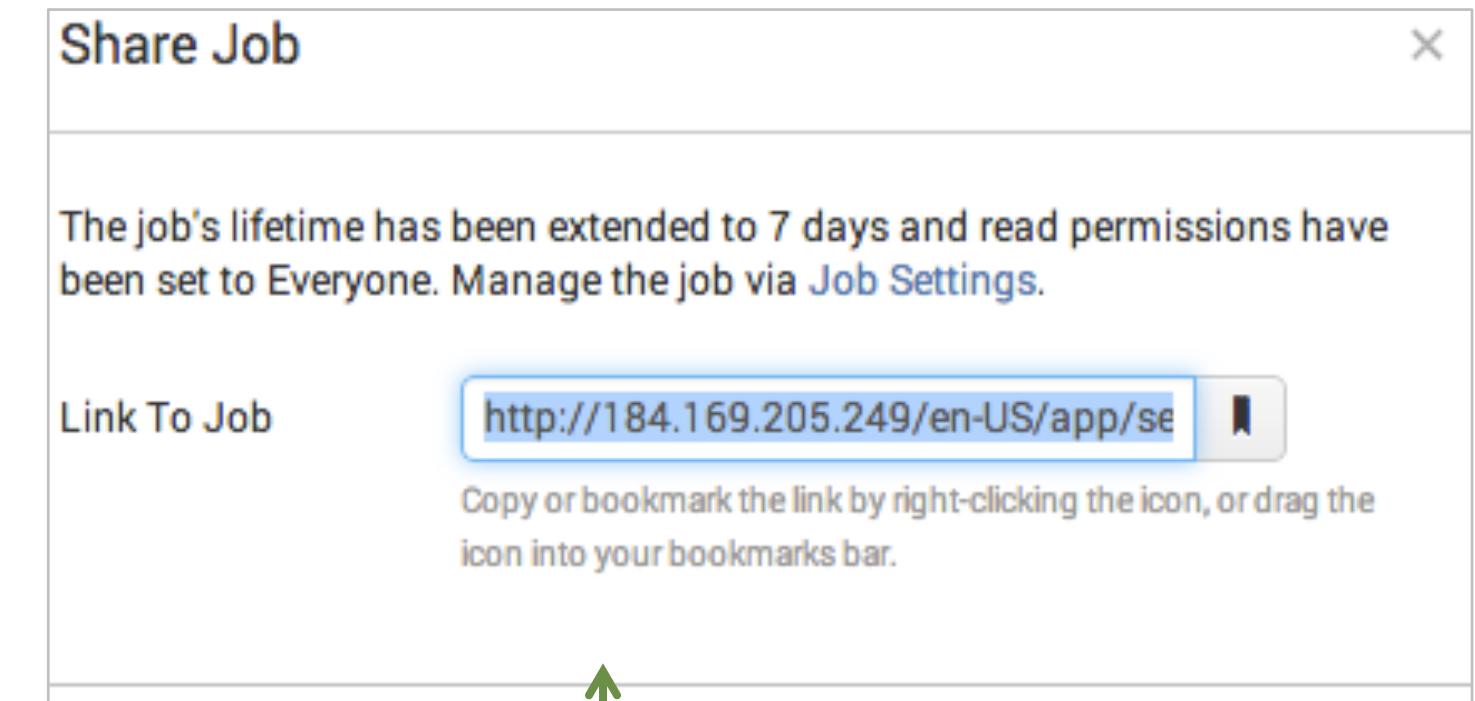
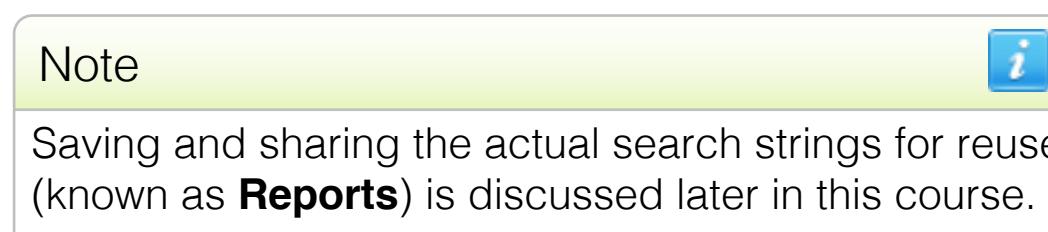
Lifetime ? 10 minutes 7 days

Link To Job <http://localhost:8008/en-US/app/search> Copy or bookmark the link by right-clicking the icon, or drag the icon into your bookmarks bar.

Cancel Save

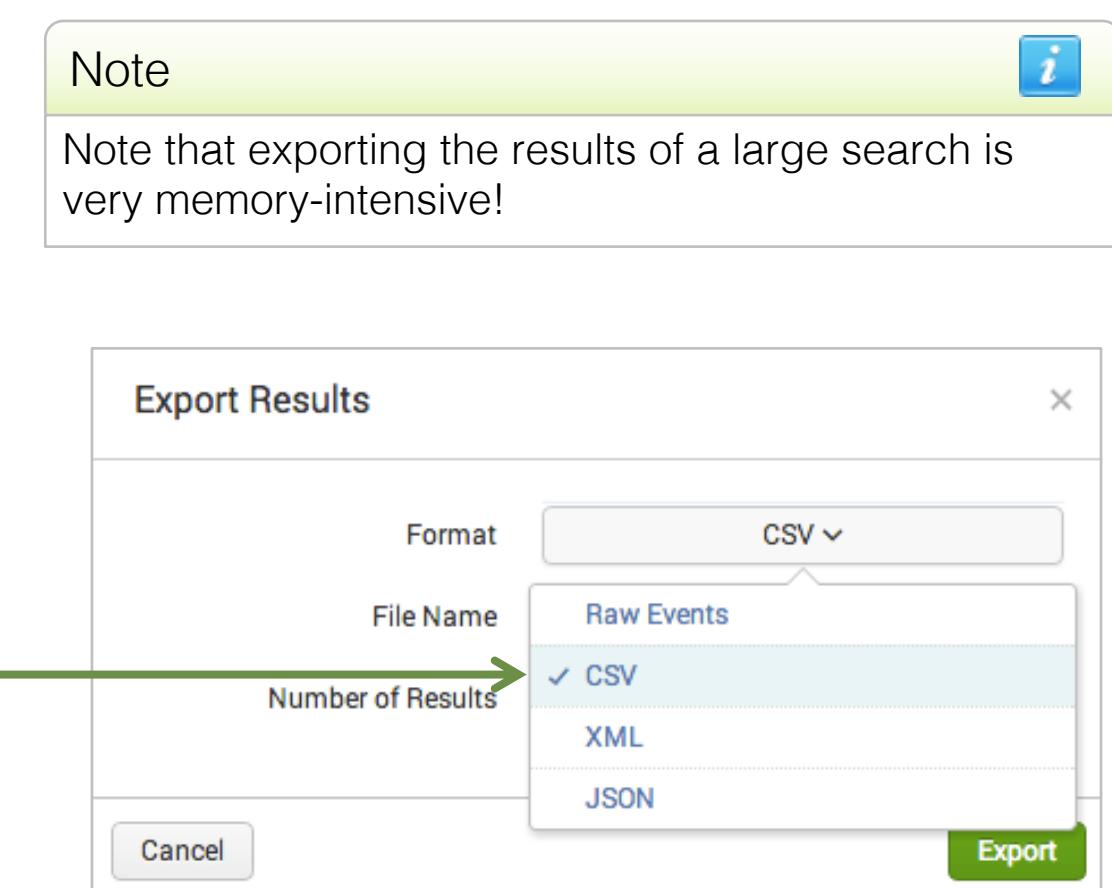
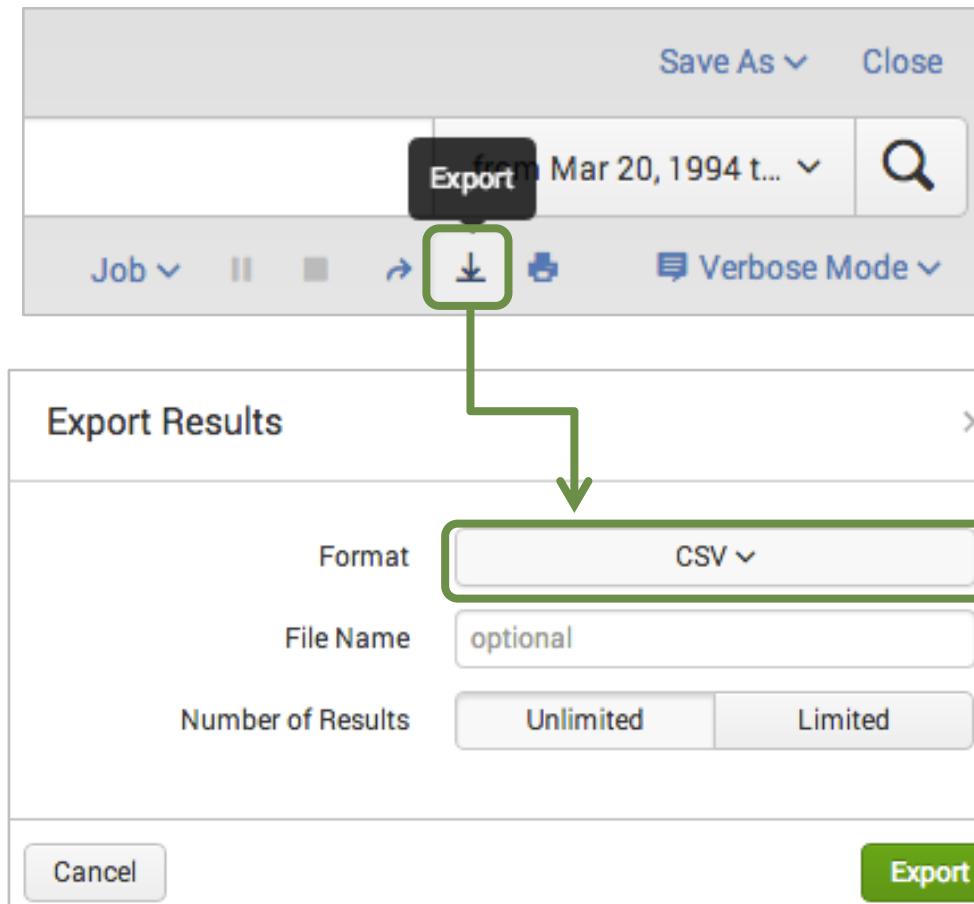
Share Search Jobs

- 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



Export Search Results

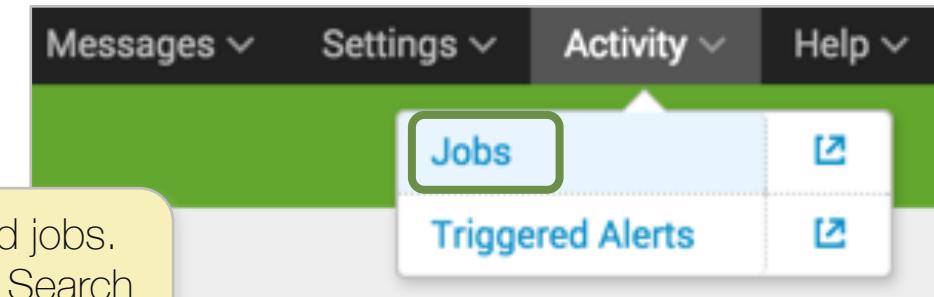
For an external copy of the results, **export** search results to Raw Events (text file), CSV, XML, or JSON format



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Review Your Job History

- Access saved search jobs from the **Activity** menu
- The Search Jobs view 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 designated app view



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

1 Jobs											App: Search & Reporting ...	Owner: All	Status: All	filter	10 Per Page
											Edit Selected				
	Owner	Application	Events	Size	Created at	Expires	Runtime	Status	Actions						
>	student16	search	67,378	13.2 MB	Oct 11, 2016 7:41:51 PM	Oct 18, 2016 7:43:45 PM	00:00:10	Done	Job	failed password	10/1/16 12:00:00.000 AM to 10/11/16 7:41:51.000 PM]				

Review Your Search History

1. Search History displays your most recent ad-hoc searches – 5 per page
2. You can set a time filter to further narrow your results

The screenshot shows the Splunk search interface with a green header bar containing 'Search', 'Pivot', 'Reports', 'Alerts', and 'Dashboards'. To the right of the header is the text 'Search & Reporting'. Below the header is a search bar with a placeholder 'enter search here...' and a dropdown menu 'All time' with a magnifying glass icon. Further down is a link 'No Event Sampling' and a 'Smart Mode' button.

The main area is divided into two sections: 'How to Search' on the left and 'What to Search' on the right. 'How to Search' includes links to 'Documentation' and 'Tutorial'. 'What to Search' shows a timeline from '5 years ago' to 'Now' with 'EARLIEST EVENT' and 'LATEST EVENT' markers. A dropdown menu for 'Search History' is open, showing options: 'No Time Filter' (selected), 'Ran: Today', 'Ran in: Last 7 Days', and 'Ran in: Last 30 Days'. Below this is a 'filter' input field and a 'No Time Filter' button.

A 'Search History' section is labeled with '1' and contains a link 'Expand your search history.' A table below shows five search entries:

	Search	Actions	Last Run
<	(sourcetype=cisco_wsa_squid OR sourcetype=access_combined) status>399 timechart count by sourcetype eval cisco_wsa_squid=cisco_wsa_squid*3 where access_combined>cisco_wsa_squid	Add to Search	a few seconds ago
>	(sourcetype=cisco_wsa_squid OR sourcetype=access_combined) status>399 timechart count by sourcetype eval...	Add to Search	Tue Apr 19 2016 15:50:07
>	sourcetype=vendor_sales VendorID < 3000 chart count over VendorStateProvince geom geo_us_states featureID...	Add to Search	Tue Apr 19 2016 15:19:55
>	sourcetype=vendor_sales VendorID < 3000 chart count over	Add to Search	Tue Apr 19 2016 15:19:43
>	sourcetype=vendor_sales VendorID < 3000 chart count by VendorStateProvince geom geo_us_states featureIDFie...	Add to Search	Tue Apr 19 2016 15:19:23

Numbered callouts point to specific elements: '1' points to the 'Expand your search history.' link, '2' points to the 'No Time Filter' button, and '3' points to the expand icon (indicated by a green square with an 'i') next to the first search entry.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module 6: Using Fields in Searches

Generated for Anil Gogia (6756585) (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
 - Examples: `host=www1 status=503`
- Fields can be searched with their names, like separating an http status code of 404 from Atlanta's area code (`area_code=404`)
- Between search terms, unless otherwise specified, **AND** is implied

The screenshot shows a search interface with four search terms listed vertically:

- area_code=404
- action=purchase status=503
- source=/var/log/messages* NOT host=mail2
- sourcetype=access_combined

A green arrow points from the text "action=purchase status=503" to the word "status".

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

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:
 - Meta fields, such as **host**, **source**, and **sourcetype**
 - Meta fields, including internal fields like **_time**, **_raw**
 - ▶ Splunk may extract other fields from the raw event data that may not be directly related to your search
- **Field discovery** is directly related to each search's results
 - Some fields in the overall data may not appear within the results of a particular search

Note 

While Splunk auto-extracts many fields, you can learn how to create your own in the *Splunk Fundamentals 2* course.

Identify Data-Specific Fields

- Data-specific fields come from the specific characteristics of your data
 - Sometimes, this is indicated by obvious key = value pairs (**action = purchase**)
 - Sometimes, this comes from data within the event, defined by the sourcetype (**status = 200**)

i	Time	Event
>	12/3/15 7:12:32.000 PM	207.36.232.245 - - [03/Dec/2015:19:12:32] "POST /cart/success.do?JSESSIONID=SD1SL3FF8ADFF4966 HTTP/1.1" 200 1443 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-26" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6" 963

Note



For more information, please see:

[Generated for Anil Gogia \(6756585\) \(C\) Splunk Inc, not for distribution](http://docs.splunk.com/Documentation/Splunk/latest/Data>Listofpretrainedsourcetypes</p></div><div data-bbox=)

Fields Sidebar

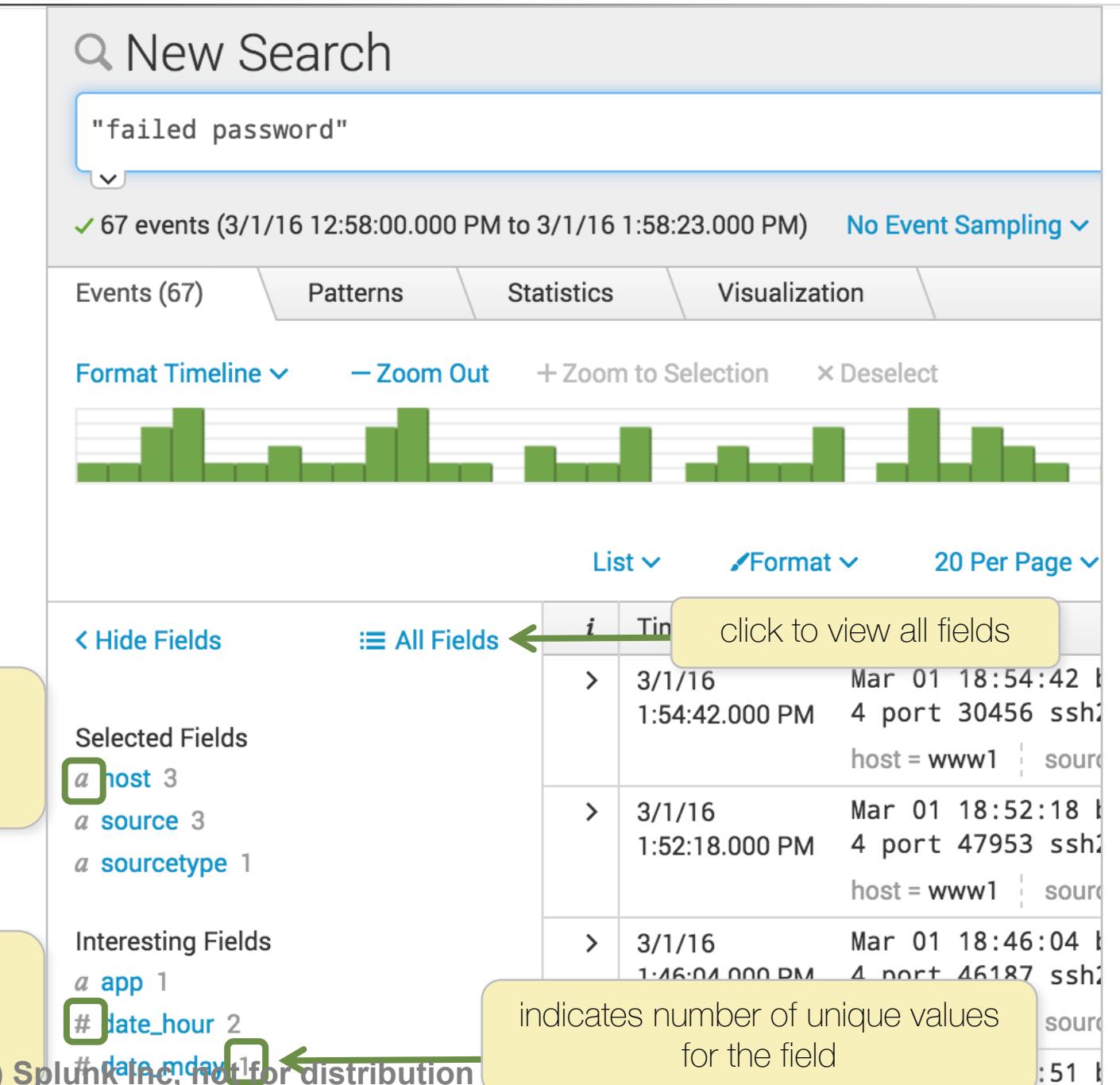
For the current search:

- **Selected Fields** – a set of configurable fields displayed for each event
- **Interesting Fields** – occur in at least 20% of resulting events
- **All Fields** link to view all fields (including non-interesting fields)

indicates the field's values are alpha-numeric

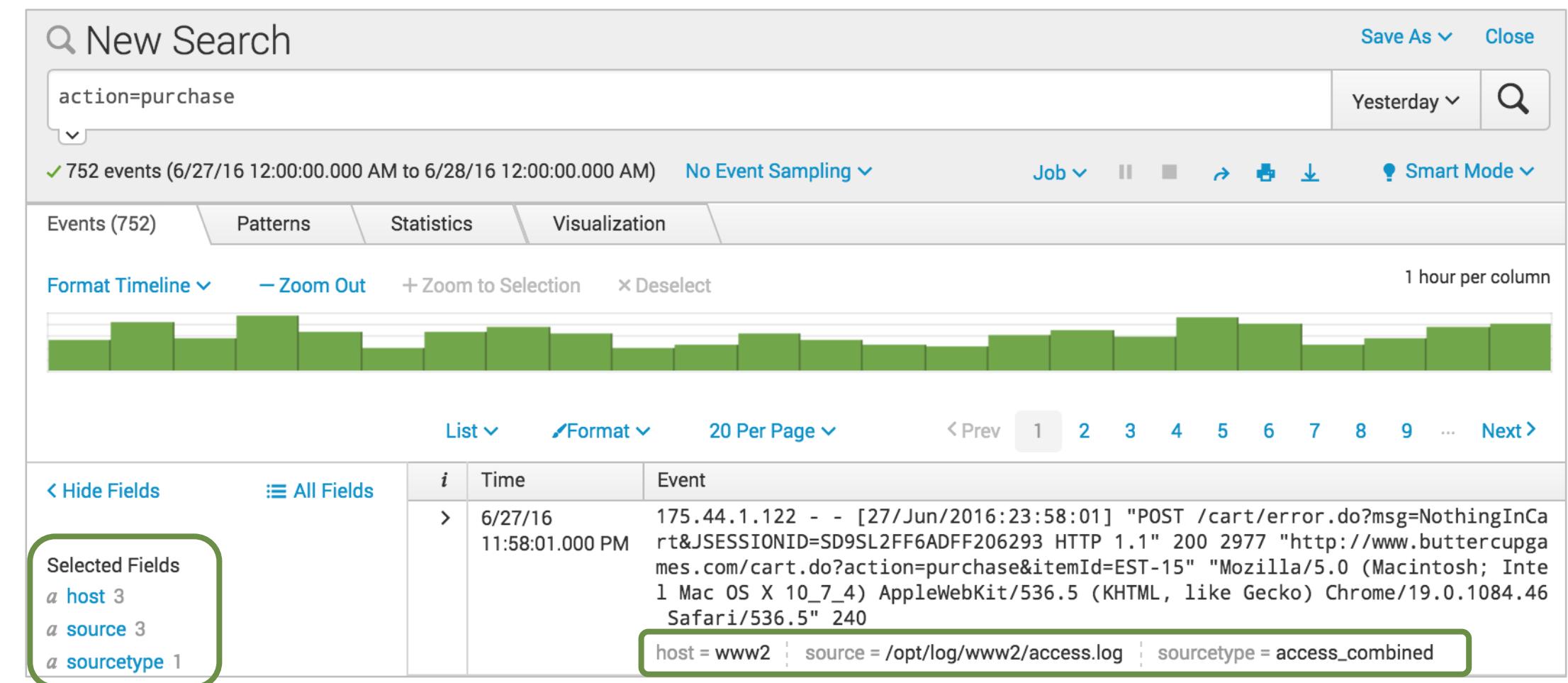
indicates that the majority of the field values are numeric

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution



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 choose any field and make it a selected field



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Make an Interesting Field a Selected Field

- You can modify selected fields

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

- Now that it is a selected field, it appears:
 - In the Selected Fields section of the Fields sidebar
 - Below each event where a value exists for that field

The screenshot shows the Splunk interface with the following components:

- Fields Sidebar:** On the left, under "Selected Fields", "action" is listed. Under "Interesting Fields", "action" is also listed with a green box around it and a red circle with the number 1 above it.
- Event Detail Dialog:** A modal window is open for an event from 2/4/16 at 3:21:43.000 PM. It shows the event details: host: 123.30.108.208, source: D3SL4FF3ADFF4964, sourcetype: http://www.buttercupgames.com. The "action" field is highlighted with a green box and a red circle with the number 2 above it.
- Event List:** Below the dialog, the main event list shows two events. The first event has its "action = purchase" value highlighted with a green box.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Make Any Field Selected

You can identify other fields as selected fields from All Fields (which shows all of the discovered fields)

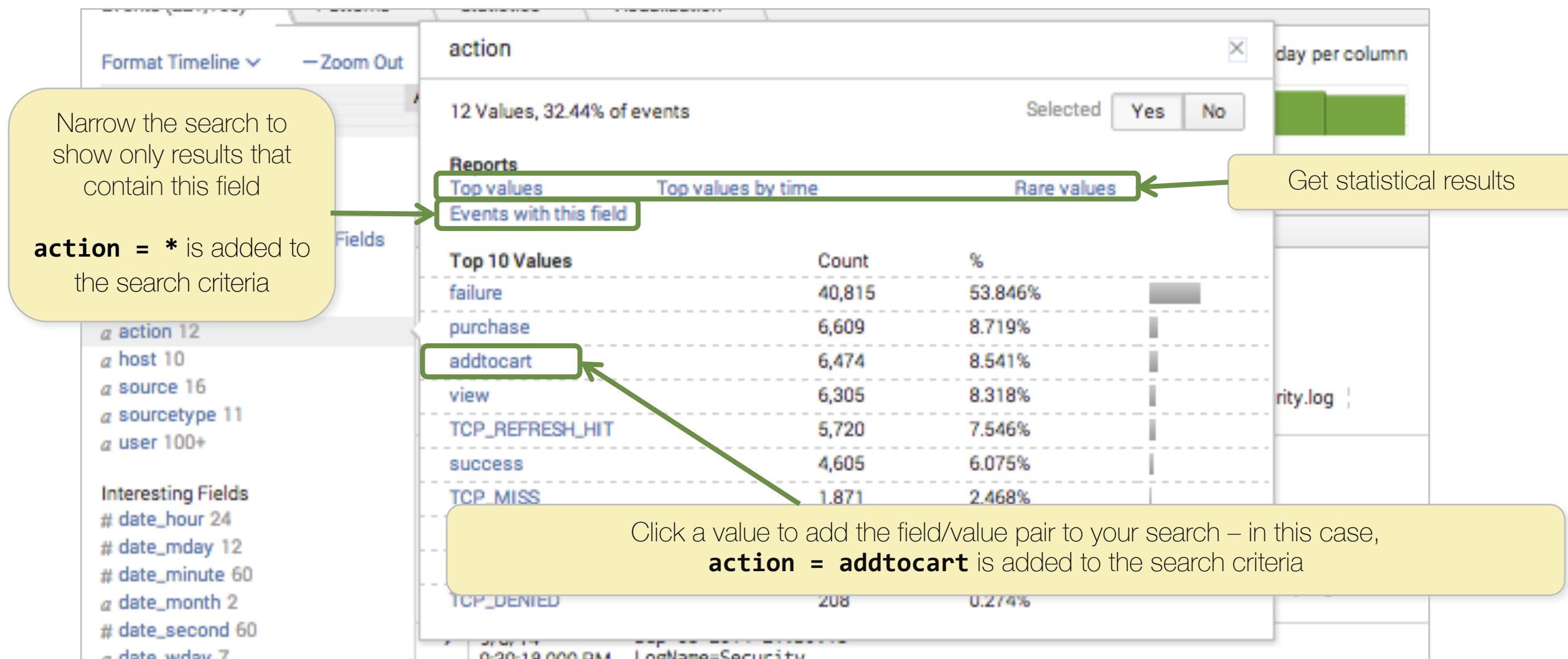
The screenshot shows the 'Select Fields' interface in Splunk. On the left, there's a sidebar with buttons for 'Hide Fields' and 'All Fields' (which is highlighted with a green box and an arrow). Below these are sections for 'Selected Fields' and a list of fields: 'action 1', 'host 3', 'source 3', and 'sourcetype 1'. The main area is a table titled 'Select Fields' with columns for 'Field', '# of Values', 'Event Coverage', and 'Type'. The table lists fields like 'action', 'host', 'source', 'sourcetype', 'JSESSIONID', 'bytes', and 'categoryId'. A filter bar at the top allows selecting fields based on coverage (1% or more) and a search bar. A tooltip at the bottom shows a selected field: 'action = purchase ; host = v ; sourcetype = access_combine'.

#	Field	# of Values	Event Coverage	Type
1	action	1	100%	String
2	host	3	100%	String
3	source	3	100%	String
4	sourcetype	1	100%	String
5	JSESSIONID	>100	100%	String
6	bytes	>100	100%	Number
7	categoryId	8	51.99%	String

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

The Field Window

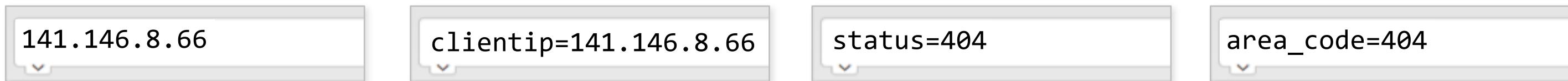
Select a field from the Fields sidebar, then:



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

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

These two searches return results

This one does not return results

Using 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
 - Example: **user=*** (to display all events that contain a value for user)

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

- Use relational operators

With numeric fields

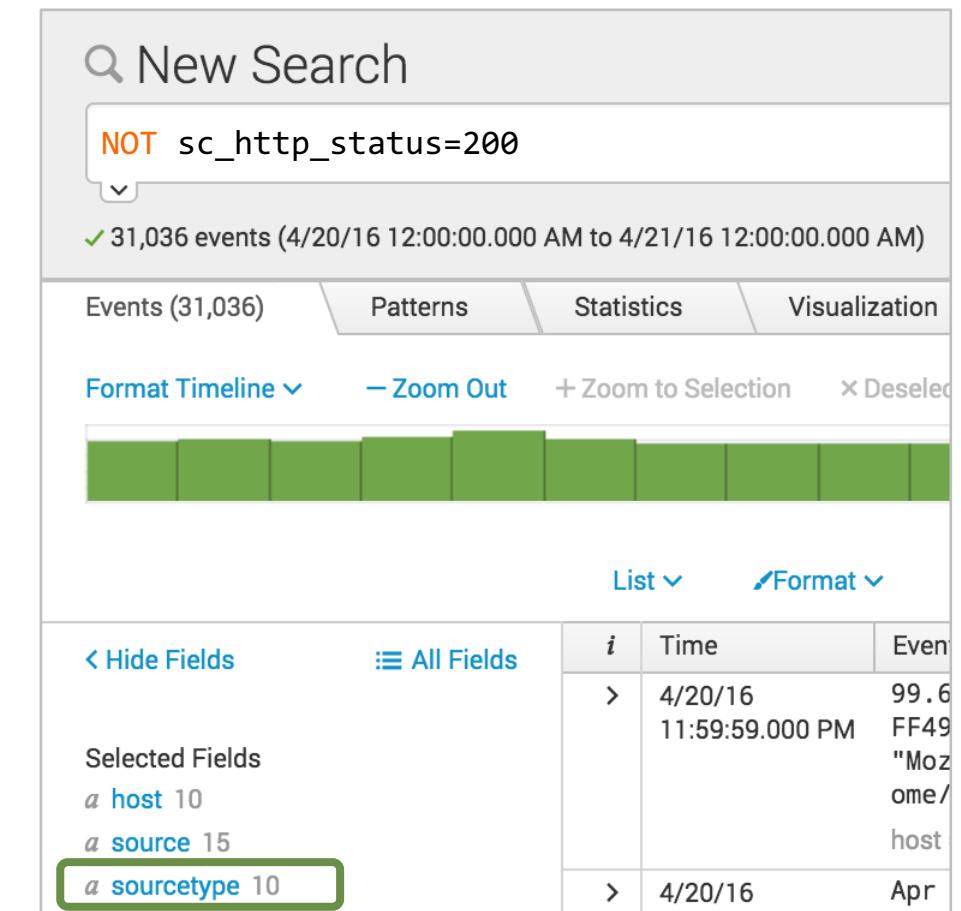
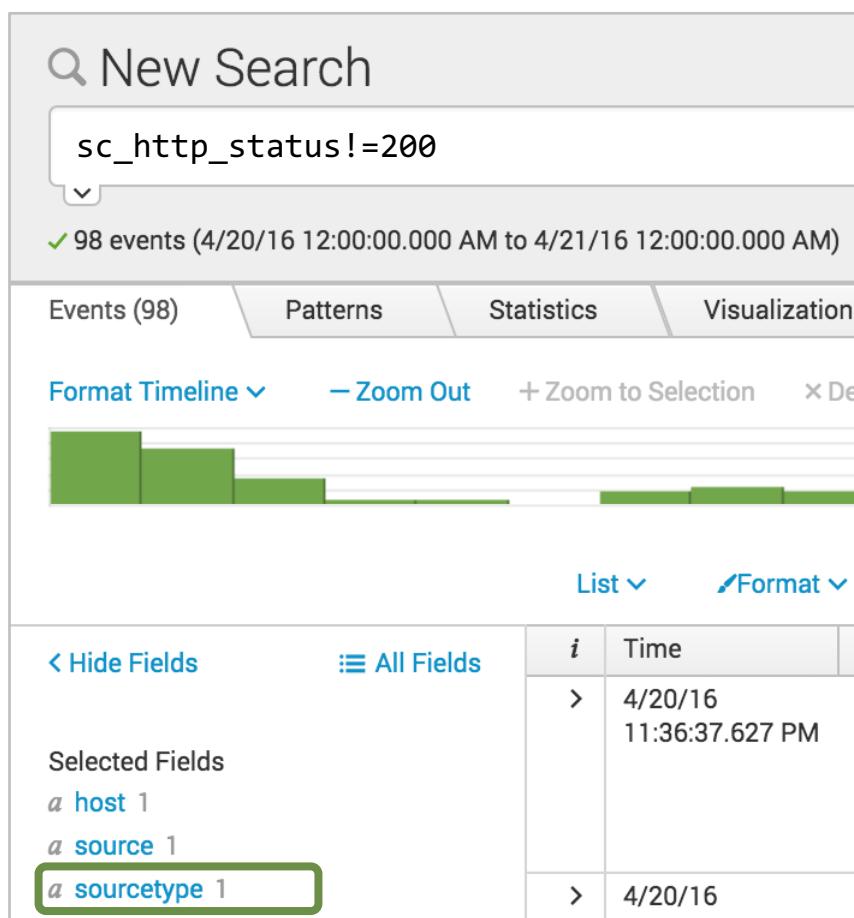
```
src_port>1000 src_port<4000
```

With alphanumeric fields

```
host!=www3
```

Example: != vs. NOT

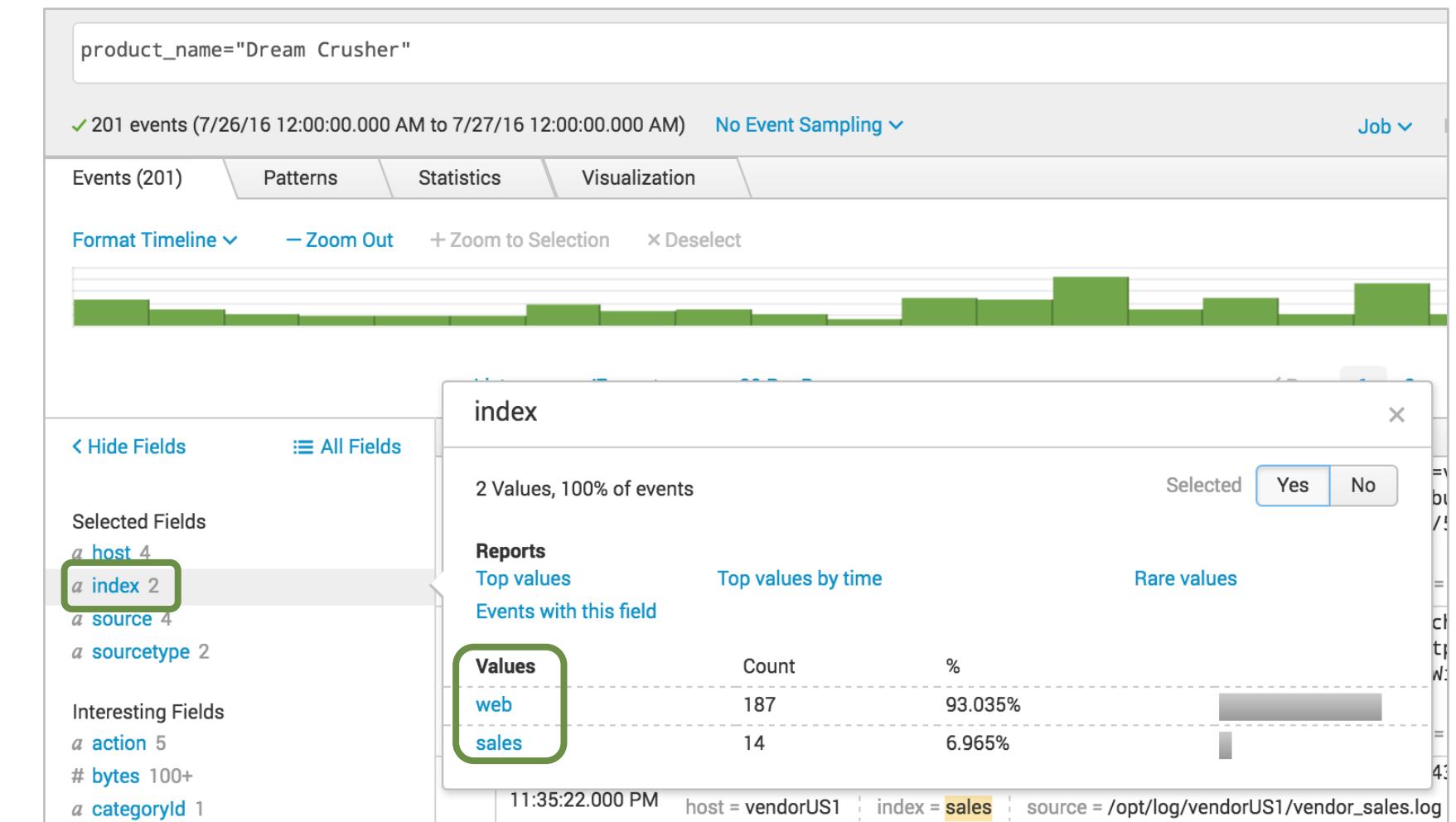
- Note that the search on the left, which uses !=, returns 98 events from one sourcetype
- The search on the right, using NOT, returns 31,036 events from *ten* sourcetypes



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Searching Against the Default Index

- In the Fields sidebar, note the **index** field
- An *index* is a location where Splunk stores – and searches for – event data
- The Splunk administrator configures the index locations that you can search, by default
- In the search shown here, data is returned from two indexes: web and sales



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Search Modes: Fast, Smart, Verbose

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 Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module 7: Best Practices for Searching

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

General Search Practices

- Time is the most efficient filter
- For best performance, specify index values at the beginning of the search string
- Be specific
 - Searching for "access denied" is always better than searching for "denied"
 - To make searches more efficient, include as many terms as possible
 - If you want to find events with "error" and "sshd" and 90% of the events include "error", but only 5% "sshd", include both values in the search
- Inclusion is generally better than exclusion
 - Searching for "access denied" is faster than NOT "access granted"

Note



Note that search terms are *case-insensitive* and search fields are *case-sensitive*.

General Search Practices (cont.)

- Filter as early as possible
 - For example, remove duplicate events, then sort
- For fastest performance, try to avoid using wildcards at the beginning of a string
- Inconsistent performance can result from using wildcards in the middle of a string, especially if the string contains punctuation or quotes

Time Range Abbreviations

- Time ranges specified in the **Advanced** tab of the time range picker
 - Time unit abbreviations include:

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

- @ symbol "snaps" to the time unit you specify
 - Snapping rounds *down* to the nearest specified unit
 - Example: Current time when the search starts is 09:37:12

-30m@h looks back to 09:00:00

Time Range: earliest and latest

- You can also specify a time range in the search bar
- To specify a beginning and an ending for a time range, use **earliest** and **latest**
- Examples:

earliest=-h

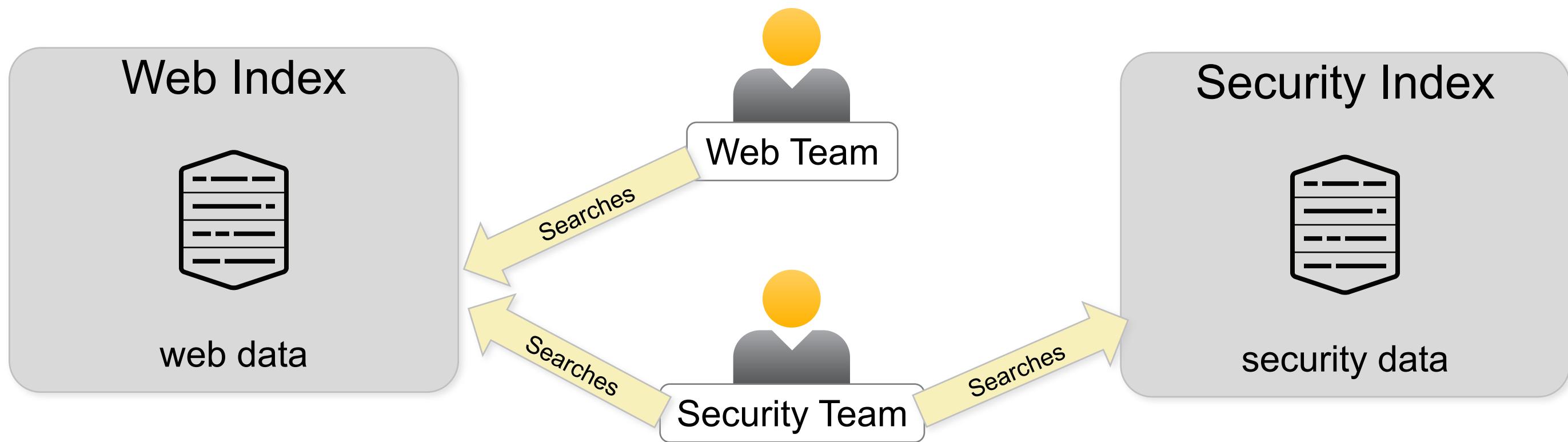
looks back one hour

earliest=-2d@d latest=@d

looks back from two days ago,
up to the beginning of today

Indexes

- An *index* is a location where Splunk stores and searches for event data



- Administrators segregate data into separate indexes to limit access by Splunk role

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Working with Indexes

- This search returns event data from the security index

The screenshot shows a Splunk search interface. The search bar contains the query `index=security "failed password"`. The results section indicates `✓ 6,193 events (8/22/16 12:00:00.000 AM to 8/23/16 12:00:00.000 AM)`. The search bar also includes a date range selector set to `Yesterday` and a search button.

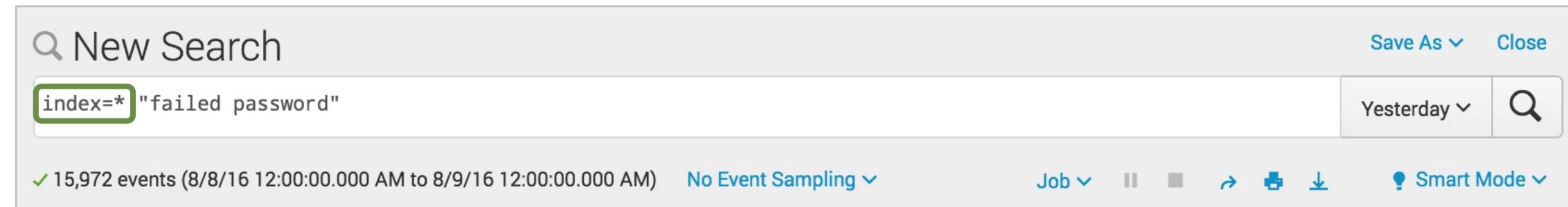
- It is possible to specify multiple index values

The screenshot shows a Splunk search interface. The search bar contains the query `(index=sales OR index=web) product_name="Dream Crusher"`. The results section indicates `✓ 241 events (10/5/16 12:00:00.000 AM to 10/6/16 12:00:00.000 AM)`. The search bar includes a date range selector set to `Yesterday` and a search button.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Working with Indexes (cont.)

It is possible to use wildcards – *, %, _, etc. – in index values



Note 1

Although `index=*` is a valid search, better performance is always obtained by specifying one or more specific index values.

Note 2

For best performance, specify the index values at the beginning of the search string.

Module 8: Splunk's Search Language

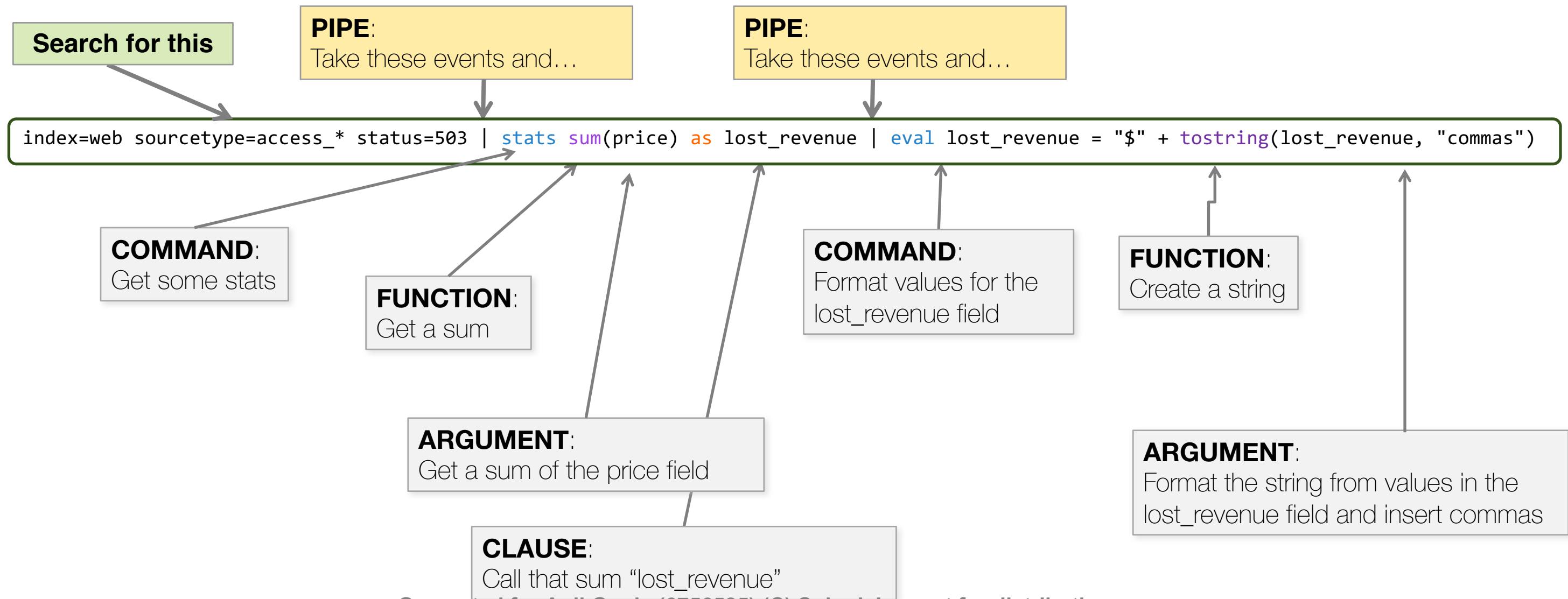
Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module Objectives

- Understand the search pipeline
- Understand search syntax concepts
- Use the table, fields and sort commands

Search Pipeline Example

This diagram represents a search, broken into its syntax components:



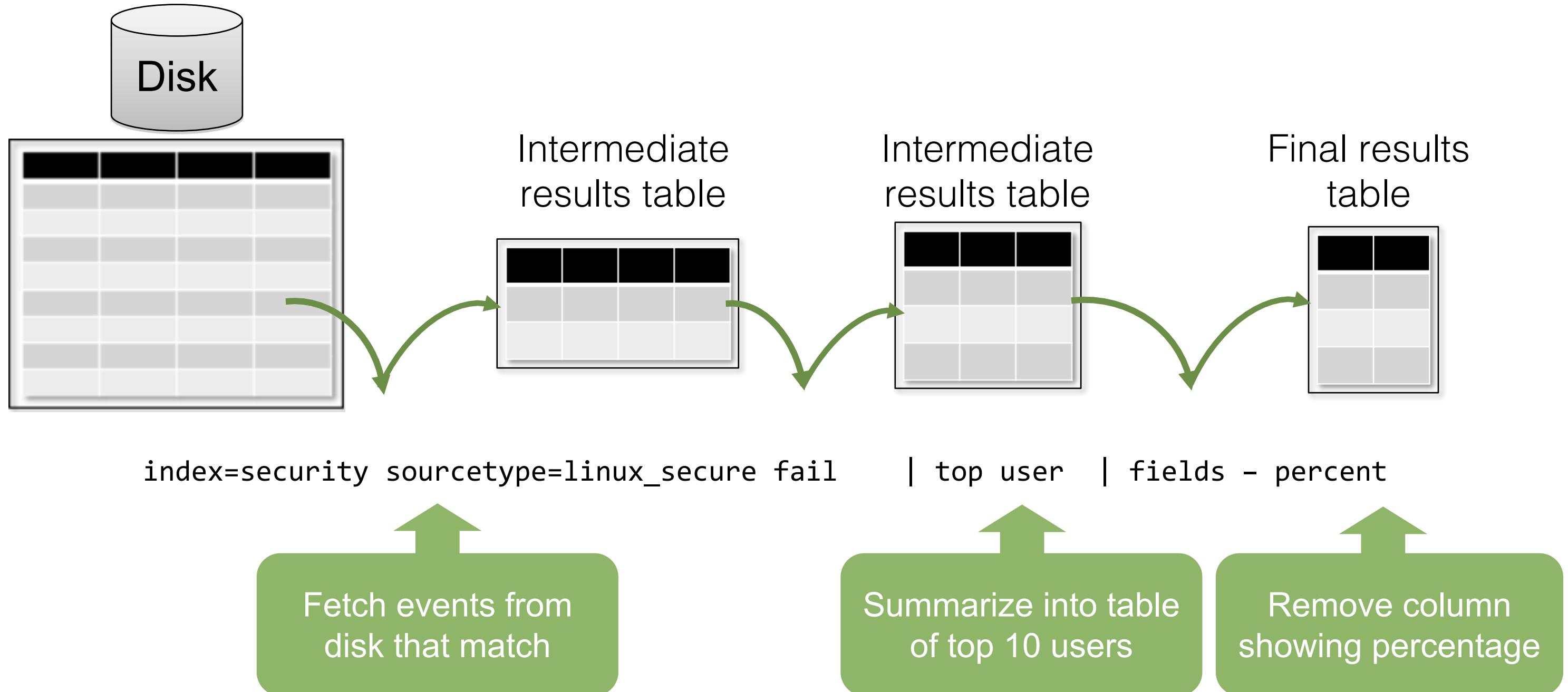
Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Search Language Syntax Concepts

Searches are made up of 5 basic components

- **Search terms** – what are you looking for?
 - Keywords, phrases, Booleans, etc.
- **Commands** – what do you want to do with the results?
 - Create a chart, compute statistics, evaluate and format, etc.
- **Functions** – how do you want to chart, compute, or evaluate the results?
 - Get a sum, get an average, transform the values, etc.
- **Arguments** – are there variables you want to apply to this function?
 - Calculate average value for a specific field, convert milliseconds to seconds, etc.
- **Clauses** – how do you want to group or rename the fields in the results?
 - Give a field another name or group values by or over

The Search Pipeline



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

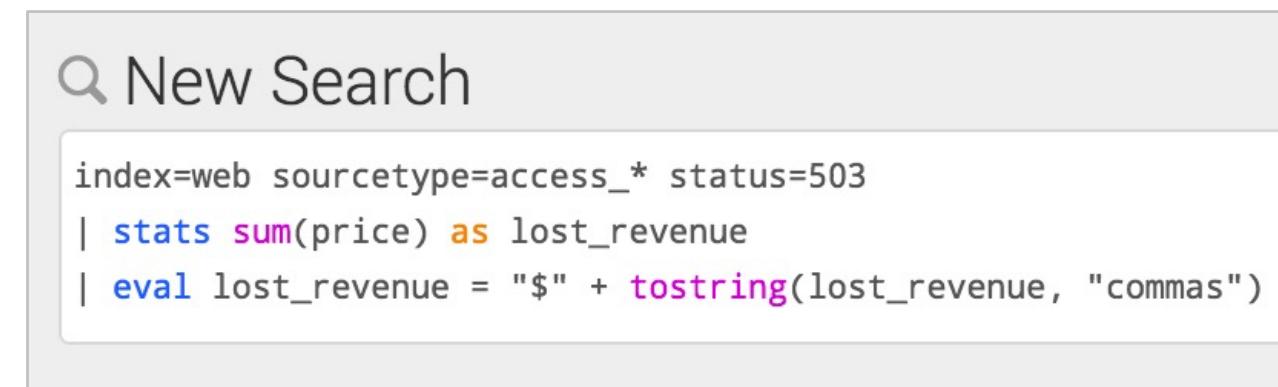
Making the Pipeline More Readable

- Clicking **Ctrl** - \ (Windows) or ⌘ - \ (MacOS) in the search box puts each pipe in the pipeline on a separate line
- For example, this:



```
index=web sourcetype=access_* status=503 | stats sum(price) as lost_revenue | eval lost_revenue = "$" + tostring(lost_revenue, "commas")
```

- Is transformed to this:

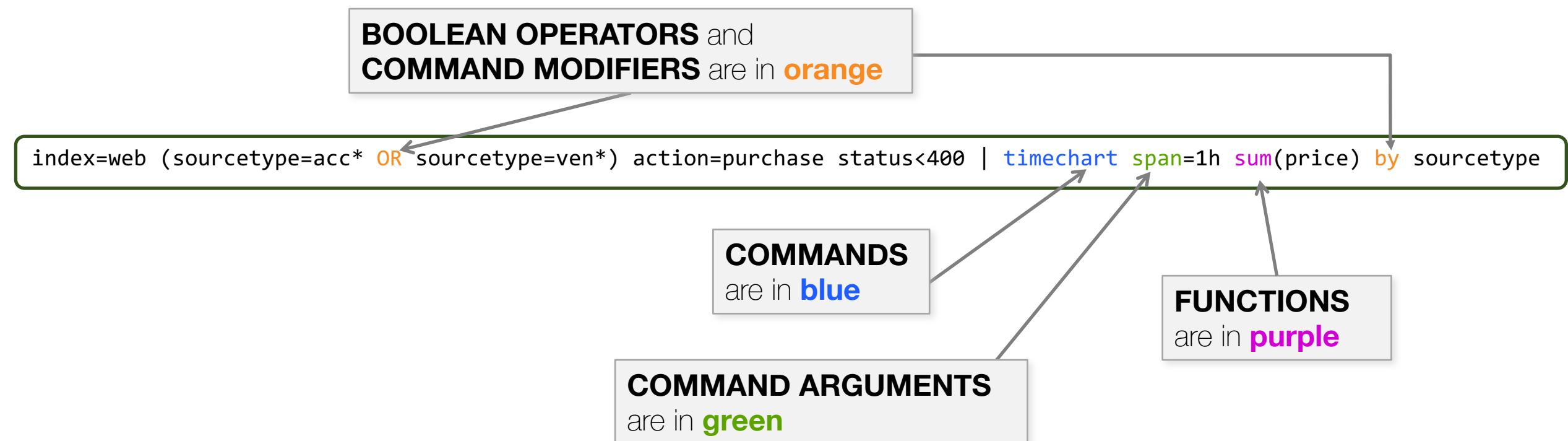


```
index=web sourcetype=access_* status=503  
| stats sum(price) as lost_revenue  
| eval lost_revenue = "$" + tostring(lost_revenue, "commas")
```

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Syntax Coloring

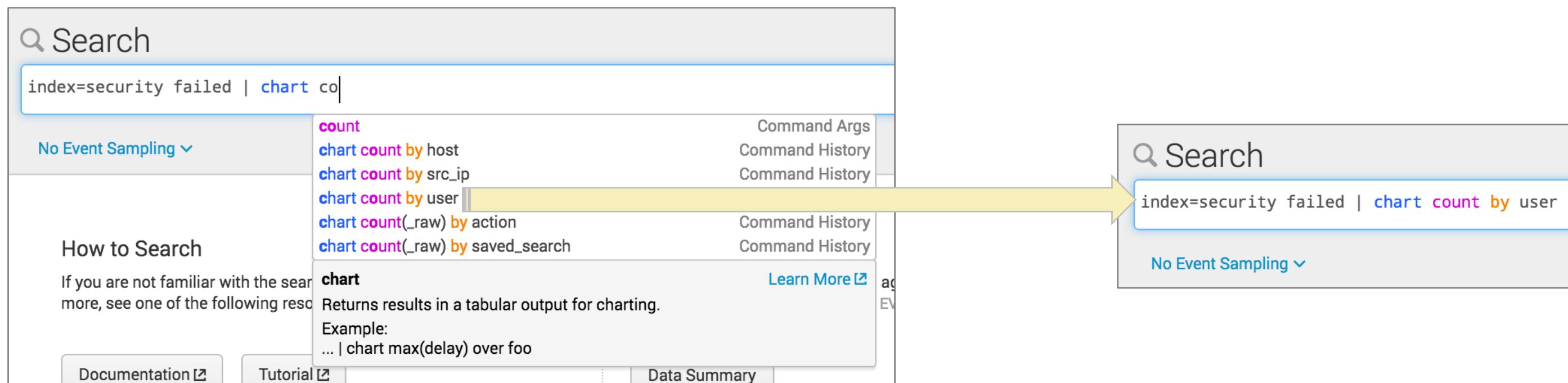
- As you type, some parts of the search string are automatically colored
- The color is based on the search syntax
 - The rest of the search string remains black



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Search Assistant

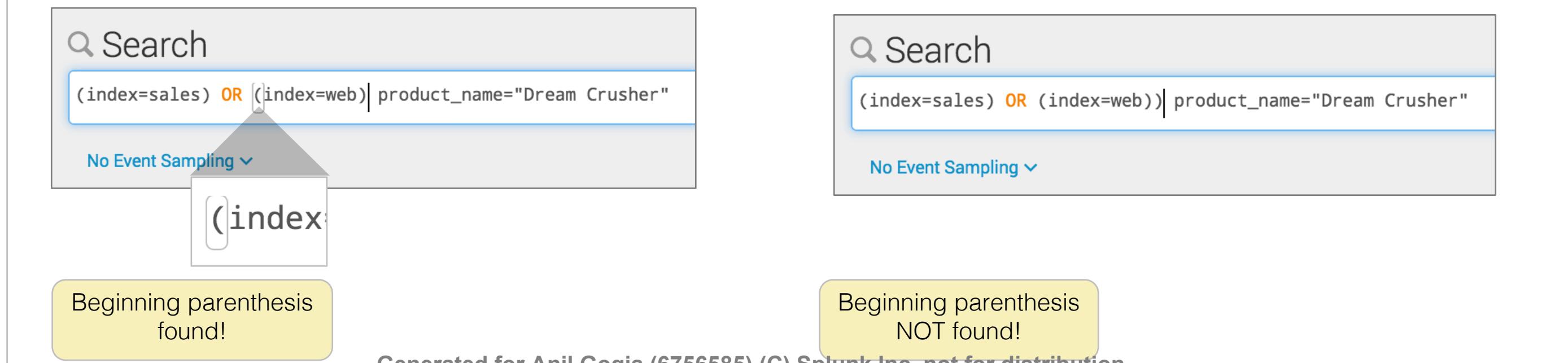
- The Search Assistant provides an autocomplete feature
- It provides convenient reminders about commands available at any given point in the search string
 - If desired, click a reminder to have its contents inserted into the search



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Search Assistant and Parentheses

- The Search Assistant provides help to match parentheses as you type
- When an end parenthesis is typed, the corresponding beginning parenthesis is automatically highlighted
 - If a beginning parenthesis cannot be found, *nothing* is highlighted



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Creating a Table

- `table` command returns a table formed by only fields in the argument list
- Columns are displayed in the order given in the command
 - Column headers are field names
 - Each row is an event
 - Rows are field values

Scenario

Display the `clientip`, `action`, `productId`, and `status` of customer interactions in the online store for the last 4 hours.

```
index=web sourcetype=access_combined  
| table clientip, action, productId, status
```

clientip	action	productId	status
223.205.219.67			200
69.80.0.18	view	WC-SH-A02	200
69.80.0.18		SF-BVS-01	408
91.205.189.15	view	FS-SG-G03	200
91.205.189.15	view	CU-PG-G06	200
91.205.189.15	view	WC-SH-A02	200
91.205.189.15	remove	WC-SH-A01	200
91.205.189.15			200

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Renaming Fields

- To change the name of a field, use the `rename` command
- Useful for giving fields more meaningful names
- When including spaces or special characters in field names, use double straight quotes:

- A `rename productId as ProductID`
- B `rename action as "Customer Action"`
- C `rename status as "HTTP Status"`

Scenario



Display the `clientip`, `action`, `productId`, and `status` of customer interactions in the online store for the last 4 hours.

```
index=web sourcetype=access_combined
| table clientip, action, productId, status
| rename productId as ProductID, A
| action as "Customer Action", B
| status as "HTTP Status" C
```

clientip	Customer Action	ProductID	HTTP Status
141.146.8.66		MB-AG-T01	200
141.146.8.66		WC-SH-A01	200
195.80.144.22		DC-SG-G02	200
141.146.8.66		WC-SH-A02	200
195.80.144.22		SC-MG-G10	200
141.146.8.66		PZ-SG-G05	200
195.80.144.22	purchase		200
195.80.144.22	purchase	SC-MG-G10	200

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

fields Command

- Field extraction is one of the most costly parts of a search
- **fields** command allows you to include or exclude specified fields in your search or report
- To include, use **fields +(default)**
 - Occurs before field extraction
 - Improves performance
- To exclude, use **fields -**
 - Occurs after field extraction
 - No performance benefit
 - Exclude fields used in search to make the table/display easier to read

fields Command – Examples

Improves performance – only the fields you specify are extracted

Scenario

Display network failures during the previous week.

Returned **6,567** results by scanning **6,567** events in **1.425** seconds:

◀ Hide Fields	≡ All Fields	<i>i</i>	Time	Event
Selected Fields		>	1/23/16 11:59:40.000 PM	Jan 18 11:28:43 bcg-payroll sshd[21263]: Failed password for root from 175.4 5.176.223 port 33307 ssh2 host = www1 source = /opt/log/www1/auth.nix sourcetype = linux_secure
		>	1/23/16 11:59:39.000 PM	Jan 17 23:59:39 bcg-fileserver sshd[9954]: Failed password for invalid user brook from 41.32.0.85 port 47187 ssh2 host = www3 source = /opt/log/www3/auth.nix sourcetype = linux_secure
Interesting Fields		>	1/23/16 11:59:37.000 PM	Jan 17 23:59:37 HOST0170 sshd[25089]: [ID 800047 auth.info] Failed publickey for naughtyuser from 23.16.0.232 port 50244 ssh2 host = www3 source = /opt/log/www3/auth.nix sourcetype = linux_secure

Scenario ?

Display network failures during the previous week. Retrieve only `user`, `app`, and `src_ip`.

```
index=security  
sourcetype=linux_secure  
(fail* OR invalid)  
| fields user, app, src_ip
```

Returned **6,567** results by scanning **6,567** events in **0.753** seconds:

Hide Fields	All Fields	<i>i</i>	Time	Event
Interesting Fields		>	1/23/16 11:59:40.000 PM	Jan 18 11:28:43 bcg-payroll sshd[21263]: Failed password for root from 175.4 5.176.223 port 33307 ssh2
app 2		>	1/23/16 11:59:39.000 PM	Jan 17 23:59:39 bcg-fileserver sshd[9954]: Failed password for invalid user brook from 41.32.0.85 port 47187 ssh2
src_ip 23		>	1/23/16 11:59:37.000 PM	Jan 17 23:59:37 HOST0170 sshd[25089]: [ID 800047 auth.info] Failed publickey for naughtyuser from 23.16.0.232 port 50244 ssh2
user 100+		>	1/23/16 11:59:10.000 PM	Jan 18 23:59:10 bcg-payroll sshd[8372]: Failed password for root from 3.0.0.44 port 37138 ssh2

Generated for Anil Gogia (6756585) (C) Splunk Inc. not for distribution

dedup Command

Use dedup to remove duplicates from your results

```
index=sales sourcetype=vendor_sales | table VendorCountry, VendorStateProvince,  
VendorCity, Vendor
```

VendorCountry	VendorStateProvince	VendorCity	Vendor
United States	Texas	Waco	Wow Games
United States	Utah	Cedar City	Woody's Games
United States	Virginia	Staunton	Woody's Games
United States	Utah	Cedar City	Woody's Games
United States	Utah	Cedar City	Woody's Games
Australia	Western Australia	Perth	Wonderland Hobbies
Australia	Western Australia	Perth	Wonderland Hobbies

```
...| dedup Vendor | table ...
```

VendorCountry	VendorStateProvince	VendorCity	Vendor
United States	Texas	Waco	Wow Games
United States	Utah	Cedar City	Woody's Games
Australia	Western Australia	Perth	Wonderland Hobbies

```
...| dedup VendorCity, Vendor | table ...
```

VendorCountry	VendorStateProvince	VendorCity	Vendor
United States	Texas	Waco	Wow Games
United States	Utah	Cedar City	Woody's Games
United States	Virginia	Staunton	Woody's Games
Australia	Western Australia	Perth	Wonderland Hobbies

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

sort Command

- Use `sort` to order your results in + ascending (default) or - descending
- To limit the returned results, use the `limit` option

```
... | sort limit=20 -categoryId, productName
```

```
... | sort 20 count
```

sort

Sorts search results by the specified fields.

Example:

```
... | sort ip, -url
```

[Learn More ↗](#)

sort Command (cont.)

sort $-/+<\text{fieldname}>$ sign followed by fieldname sorts results in the sign's order

sort $-/+ <\text{fieldname}>$ sign followed by space and then fieldname applies sort order to all following fields without a different explicit sort order

```
index=sales sourcetype=vendor_sales
| dedup Vendor
| sort - VendorCountry, +VendorStateProvince, VendorCity, Vendor
| table VendorCountry, VendorStateProvince, VendorCity, Vendor
```

VendorCountry	VendorStateProvince	VendorCity	Vendor
United States	Arizona	Yuma	Yumster Games
United States	Arizona	Tucson	Boothill Games
United States	Arizona	Phoenix	Rising Games
United States	Arizona	Phoenix	Phoenix Games
United States	Arizona	Flagstaff	Flaggin Games

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module 9: Transforming Commands

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module Objectives

Identify and use the following commands and their functions:

- top
- rare
- Stats
- dedup

Getting Top Values

- The top command finds the most common values of a given field in the result set
 - By default, returns top 10 results

src_ip	count	percent
10.3.10.46	53	19.629630
10.2.10.163	50	18.518519
10.1.10.172	43	15.925926
87.194.216.51	23	8.518519
217.132.169.69	19	7.037037
188.143.232.202	11	4.074074
69.80.0.18	10	3.703704
216.221.226.11	9	3.333333
142.233.200.21	8	2.962963
84.34.159.23	7	2.592593

Scenario

During the last 60 minutes, which IP addresses generated the most attacks?

```
index=security sourcetype=linux_secure  
(fail* OR invalid)  
| top src_ip
```

top Command

- By default, output displays in table format
- Automatically returns **count** and **percent** columns
- Common constraints:
`limit countfield showperc`

Note



Refer to docs.splunk.com for the other available options.

top

[Learn More ↗](#)

Displays the most common values of a field.

Example:

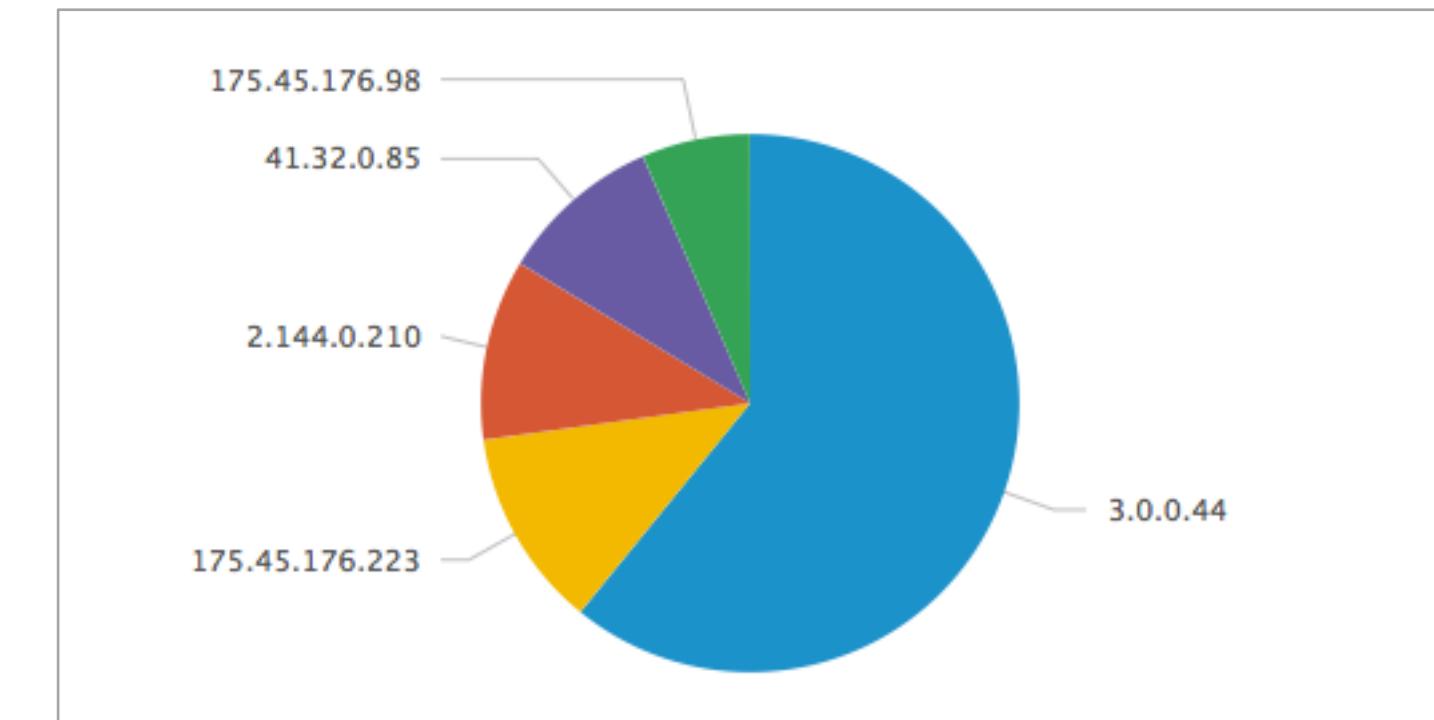
`... | top limit=20 url`

top Command – Single Field Example

- `limit=#` returns this number of results
- By default, 10 results are displayed
- `limit=0` returns unlimited results

```
sourcetype=linux_secure index=security  
(fail* OR invalid)  
| top limit=5 src_ip
```

Scenario		
src_ip	count	percent
10.2.10.163	73	27.037037
10.1.10.172	42	15.555556
10.3.10.46	41	15.185185
87.194.216.51	19	7.037037
12.130.60.4	17	6.296296



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

top – Multiple Field Example

- If the `showperc` is not included – or it is included and set to `t` – a **percent** column is displayed
- If `showperc=f`, then a percent column is NOT displayed

Scenario ?
Display the top 3 common values for users and web categories browsed during the last 24 hours.

```
index=network sourcetype=cisco_wsa_squid  
| top user A x_webcat_code_full limit=3 B
```

user	x_webcat_code_full	count	percent
apucci@buttercupgames.com	Games	79	6.152648
arangel@buttercupgames.com	Society and Culture	61	4.750779
rerde@buttercupgames.com	Arts and Entertainment	54	4.205607

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

top – Single Field with by Clause Example

Scenario



Display the top 3 common web categories browsed by each user during the last 24 hours.

```
index=network sourcetype=cisco_wsa_squid  
| top x_webcat_code_full B by user A limit=3
```

user	x_webcat_code_full	count	percent
acurry@buttercupgames.com	Uncategorized URLs	10	71.428571
acurry@buttercupgames.com	Sports and Recreation	1	7.142857
acurry@buttercupgames.com	Society and Culture	1	7.142857
adombrowski@buttercupgames.com	Computers and Internet	2	33.333333
adombrowski@buttercupgames.com	Spiritual Healing	1	16.666667
adombrowski@buttercupgames.com	Shopping	1	16.666667

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

top – Specifying Options

- By default, the value of the **countfield** is **count**
- **countfield=string** provides the name of a new field to write the count value

Scenario ?

Display the top 3 user/web categories browsed combinations during the last 24 hours. Rename the count field and show count, but not the percentage.

```
index=network sourcetype=cisco_wsa_squid  
| top user x_webcat_code_full limit=3 A  
countfield="Total Viewed" B showperc=f
```

user	x_webcat_code_full	Total Viewed
apucci@buttercupgames.com	A Games	B 79
arangel@buttercupgames.com	Society and Culture	61
rerde@buttercupgames.com	Arts and Entertainment	54

Note i

A Boolean can be t/f, true/false, as well as 1/0.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

rare Command

- The **rare** command returns the least common field values of a given field in the results
- Options are identical to the **top** command

Scenario ?

Which product is the least sold by Buttercup Games vendors over the last 60 minutes?

```
index=sales sourcetype=vendor_sales  
| rare product_name showperc=f limit=1
```

Events	Patterns	Statistics (1)	Visualization
20 Per Page ▾	Format ▾	Preview ▾	
product_name ◊			<input type="text"/> count ◊ <input type="text"/>
Fire Resistance Suit of Provolone			1

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

stats Command

- **stats** enables you to calculate statistics on data that matches your search criteria
- Common functions include:
 - **count** – returns the number of events that match the search criteria
 - **distinct_count**, **dc** – returns a count of unique values for a given field
 - **sum** – returns a sum of numeric values
 - **avg** – returns an average of numeric values
 - **list** – lists all values of a given field
 - **values** – lists unique values of a given field

Note



To view all of the functions for **stats**, please see:

<http://docs.splunk.com/Documentation/Splunk/Latest/SearchReference/CommonStatsFunctions>

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

stats Command – count

- count returns the number of matching events based on the current search criteria
- Use the as clause to rename the count field

Scenario ?
Count the invalid or failed login attempts during the last 60 minutes.

```
index=security sourcetype=linux_secure  
(invalid OR failed)  
| stats count
```

```
index=security sourcetype=linux_secure  
(invalid OR failed)  
| stats count as "Potential Issues"
```

Events	Patterns	Statistics (1)	Visualization
10 Per Page ▾	✓Format ▾	Preview ▾	
count ◊			✎
63			

Events	Patterns	Statistics (1)	Visualization
10 Per Page ▾	✓Format ▾	Preview ▾	
Potential Issues ◊			✎
63			

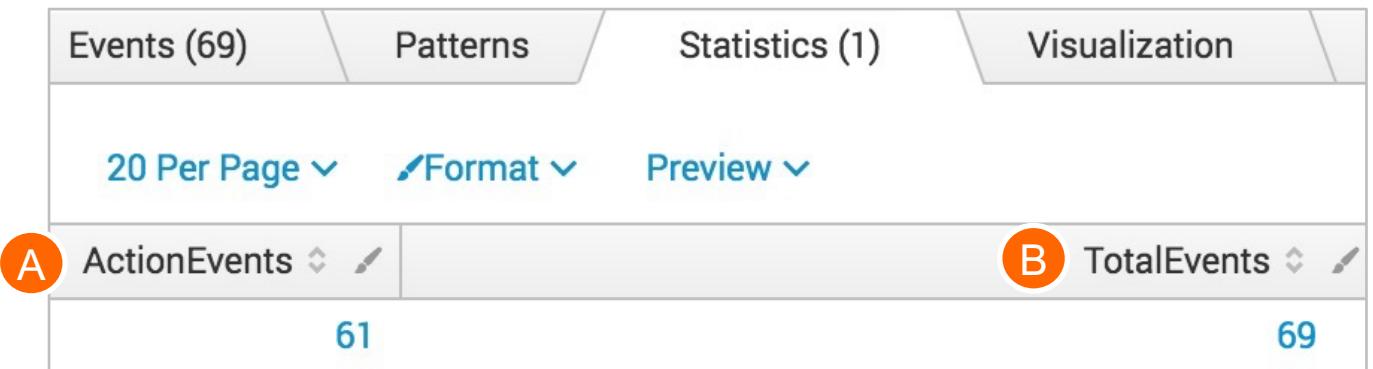
Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

stats Command – count(*field*)

Adding a *field* as an argument to the **count** function returns the number of events where a value is present for the specified field

Scenario ?
Count the number of events during the last 15 minutes that contain a vendor action field. Also count the total events.

```
index=security sourcetype=linux_secure  
| stats count(vendor_action) as ActionEvents,  
  count as TotalEvents A B
```



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

stats Command – by *fields*

Scenario



Count the number of events by user, app, and vendor action during the last 15 minutes.

```
index=security sourcetype=linux_secure  
| stats count by user, app, vendor_action
```

- **by clause** returns a count for each value of a named field or set of fields
- Can use any number of fields in the **by *field*** list

user	app	vendor_action	count
abc	sshd	Failed	1
admin	sshd	Failed	4
administrator	sshd	Failed	1
alex	sshd	Failed	1
apache	sshd	Failed	1
backup	sshd	Failed	1
ben	sshd	Failed	1
bin	sshd	Failed	2
britany	sshd	Failed	1
daemon	sshd	Failed	1

stats Command – distinct_count(*field*)

- **distinct_count()** or **dc()** provides a count of how many unique values there are for a given field in the result set
- This example counts how many unique values for **s_hostname**

Scenario ?
How many unique websites have our employees visited in the last 4 hours?

```
index=network sourcetype=cisco_wsa_squid  
| stats dc(s_hostname) as "Websites visited:"
```

The screenshot shows a search interface with the following details:

- Header tabs: Events, Patterns, Statistics (1), Visualization.
- Search parameters: 20 Per Page, Format, Preview.
- Search results table:
 - Column: Websites visited:
 - Value: 25

stats Command – sum(*field*)

Scenario ?

How much bandwidth did employees spend at each website during the past week?

```
index=network sourcetype=cisco_wsa_squid
| stats sum(sc_bytes) as Bandwidth by s_hostname
| sort -Bandwidth
```

For fields with a numeric value, you can sum the actual values of that field

The screenshot shows a Splunk search results page. At the top, there are tabs for Events, Patterns, Statistics (54), and Visualization. The Statistics tab is selected. Below the tabs are filters: 20 Per Page, Format, and Preview. The main area displays a table with two columns: s_hostname and Bandwidth. The table lists six websites with their corresponding bandwidth values. The table is highlighted with a green border.

s_hostname	Bandwidth
www.gctsindia.in	4866091
www.heals.co.uk	1233522
www.animationmagazine.net	1203433
www.kare11.com	1202753
www.finedinings.com	747407

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

stats Command – sum(*field*) – (cont.)

Scenario



Report the number of retail units sold and sales revenue for each product during the previous week.

```
index=sales sourcetype=vendor_sales
```

```
| stats A count(price) as "Units Sold"
```

```
B sum(price) as "Total Sales" by product_name C
```

```
| sort -"Total Sales" D
```

- A A single **stats** command
- B can have multiple functions
- C The **by** clause is applied to both functions
- D **sort** Total Sales in descending order

product_name	Units Sold	Total Sales
Dream Crusher	A 73	B 2919.27
Manganiello Bros.	53	2119.47
World of Cheese	66	1649.34
SIM Cubicle	81	1619.19
Orvil the Wolverine	35	1399.65
Final Sequel	49	1224.51
Mediocre Kingdoms	42	1049.58
Curling 2014	48	959.52
Benign Space Debris	25	624.75
Manganiello Bros. Tee	62	619.38

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

stats Command – avg(*field*)

- The **avg** function provides the average numeric value for the given numeric field
- An event is not considered in the calculation if it:
 - Does not have the field
 - Has an invalid value for the field

Scenario ?
What is the average bandwidth used for each website usage type?

```
index=network sourcetype=cisco_wsa_squid  
| stats avg(sc_bytes) as "Average Bytes" A  
by usage B
```

usage	Average Bytes
Borderline	13553.723173
Business	11277.155763
Personal	14874.552763 A
Unknown	10724.935021
Violation	8982.340426

stats Command – *list(field)*

- **list** function lists all field values for a given field
- This example lists the websites visited by each employee
 - Security logs generate an event for each network request
 - This causes the same hostname to appear multiple times
 - To return a list of “unique” field values, use the **values** function

Scenario



Which websites has each employee accessed during the last 60 minutes?

```
index=network sourcetype=cisco_wsa_squid  
| stats list(s_hostname) as "Websites visited:"  
by cs_username
```

cs_username	Websites visited:
basselin@buttercupgames.com	- -
blu@buttercupgames.com	www.lowermybills.com
cquinn@buttercupgames.com	- static.pochta.ru
dhalo@buttercupgames.com	-
dpiazza@buttercupgames.com	www.ayles.com www.ayles.com www.ayles.com www.ayles.com www.ayles.com www.ayles.com

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

stats Command – values(*field*)

Scenario



Display by IP address the names of users who have failed access attempts in the last 60 minutes.

```
index=security sourcetype=linux_secure fail*
| stats values(user) as "User Names",
  count(user) as Attempts by src_ip
```

values function lists unique values for the specified field

src_ip	User Names	Attempts
1.0.32.67	root	2
10.232.44.142	twilliam	1
10.232.44.71	jsimon1	1
175.45.176.223	gbottazzi oracle root scanner user	37
175.45.176.98	abc andrew cvs enquiries logs michael test test3	8

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module 10: Creating Reports and Dashboards

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module Objectives

- Save a search as a report
- Edit a report
- Create reports that display statistics (tables) or visualizations (charts)
- Create a dashboard
- Add a report to a dashboard
- Add a pivot to a dashboard
- Edit a dashboard

Reports

- Reports are saved searches
- Reports can show events, statistics (tables), or visualizations (charts)
- 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
- There are two ways to create a report: pivot or search

Smart Naming

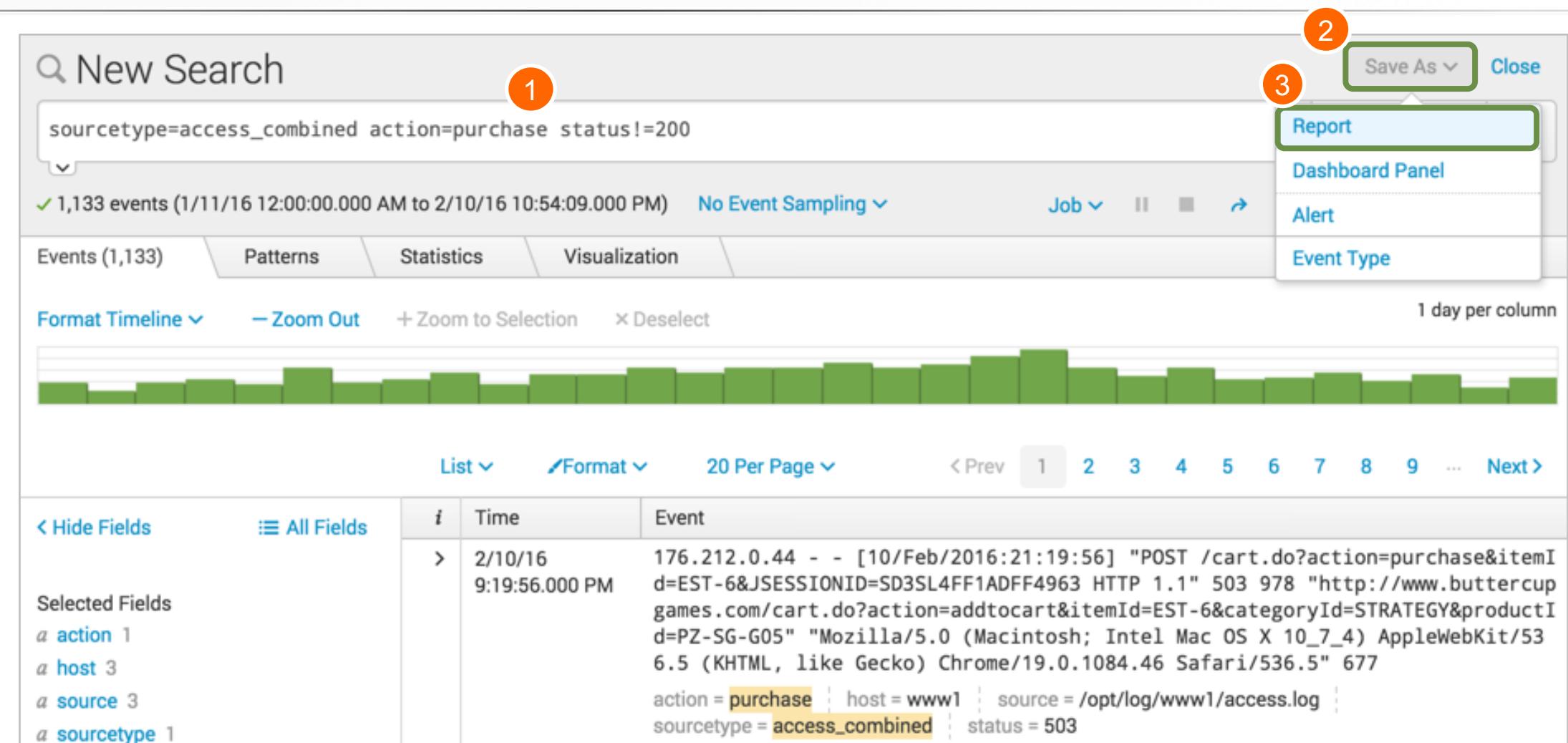
- Before you begin using Splunk on the job, define a naming convention so you can always find your reports and tell them apart
- For example, you can create something simple like this:
 - <group>_<object>_<description>
 - **group**: the name of the group or department using the knowledge object such as sales, IT, finance, etc.
 - **object**: report, dashboard, macro, etc.
 - **description**: WeeklySales, FailedLogins, etc.
 - Using this example, a quarterly sales report can be identified as:
 - Sales_Report_QuarterlySalesRevenue

Note

If you set up naming conventions early in your implementation, you can avoid some of the more challenging object naming issues. The example is a suggestion. The details are found in the Splunk product documentation:
<http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Developnamingconventionsforknowledgeobjects>

Create a Report from Search

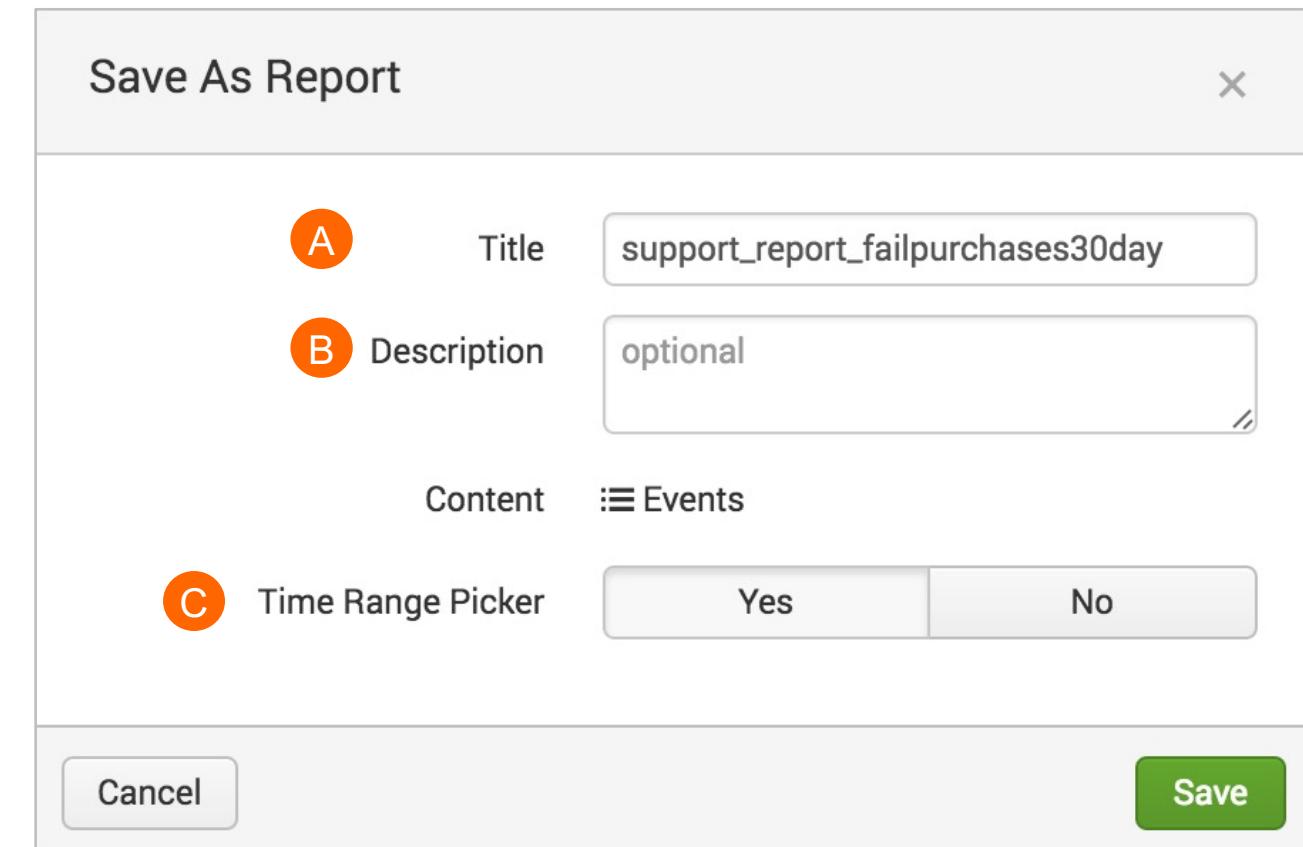
- 1 Run a search
- 2 Select **Save As**
- 3 Select **Report**



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Create a Report from Search (cont.)

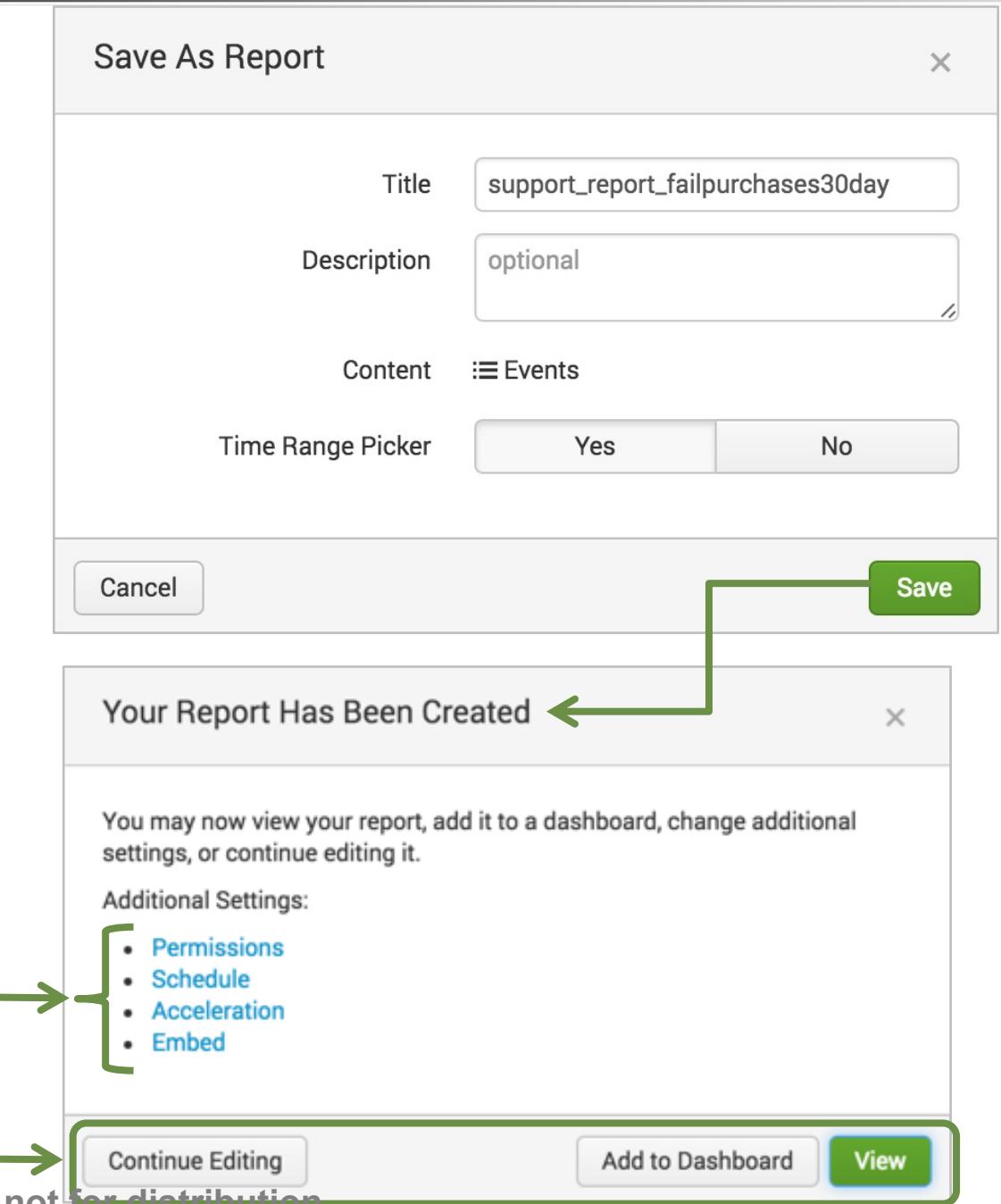
- A Give the report a meaningful title (required)
- B Specify a description (optional)
- C Select whether to include or not to include a time range picker
 - The report will be saved with the time range that was selected when it was created
 - Adding a time range picker allows you to adjust the time range of the report when you run it



Create a Report from Search (cont.)

You can change Additional Settings, as well as use the dialog buttons:

- Click **Continue Editing** to make changes to your report
- Click **Add to Dashboard** to add your report to a dashboard
- Click **View** to display your report or run it again



Additional Settings

Dialog buttons

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)

support_report_failpurchases30day

Edit More Info Add to Dashboard

Last 30 days

✓ 2,866 events (5/22/16 12:00:00.000 AM to 6/21/16 2:42:37.000 AM)

Job ▾ II ⌂ ⌃ + ⌄

20 per page ▾ < Prev 1 2 3 4 5 6 7 8 9 ... Next >

i	Time	Event
>	6/21/16 1:27:56.000 AM	217.23.14.61 - - [21/Jun/2016:01:27:56] "POST /cart.do?action=purchase&itemId=EST-26&JSESSIONID=SD8SL2FF3ADFF4965 HTTP 1.1" 503 3803 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-26&categoryId=ARCADE&productId=MB-AG-G07" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 949 host = www1 source = /opt/log/www1/access.log sourcetype = access_combined
>	6/21/16 1:13:00.000 AM	128.241.220.82 - - [21/Jun/2016:01:13:00] "POST /cart.do?action=purchase&itemId=EST-12&JSESSIONID=SD10SL3FF2ADFF4958 HTTP 1.1" 503 2917 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-12&categoryId=S TRATEGY&productId=DC-SG-G02" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 871 host = www2 source = /opt/log/www2/access.log sourcetype = access_combined

All Yours This

i Title ^

> Errors in the last 24 hours

> Errors in the last hour

> License Usage Data Cube

> Orphaned scheduled searches

> support_report_failpurchases30day

Open in Search Edit nobody search App

Open in Search Edit student16 search Private

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Editing 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
- Additionally, you can clone or delete the report

The screenshot shows a Splunk search results page for a report named "support_report_failpurchases...". The search query is:

```
sourcetype=access_combined action=purchase status!=200
```

The results show 2,866 events from May 22, 2016, to June 21, 2016. A context menu is open on the right side of the screen, listing options: Edit, More Info, Add to Dashboard, Open in Search, Edit Description, Edit Permissions, Edit Schedule, Edit Acceleration, Clone, Embed, and Delete. The "Delete" option is highlighted with a yellow box.

Report details:

- Last 30 days
- 20 per page
- Time Event
- 6/21/16 217.23.14.6 1:27:56.000 AM 4965 HTTP 1 DE&productI Chrome/19.0 host = www1

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

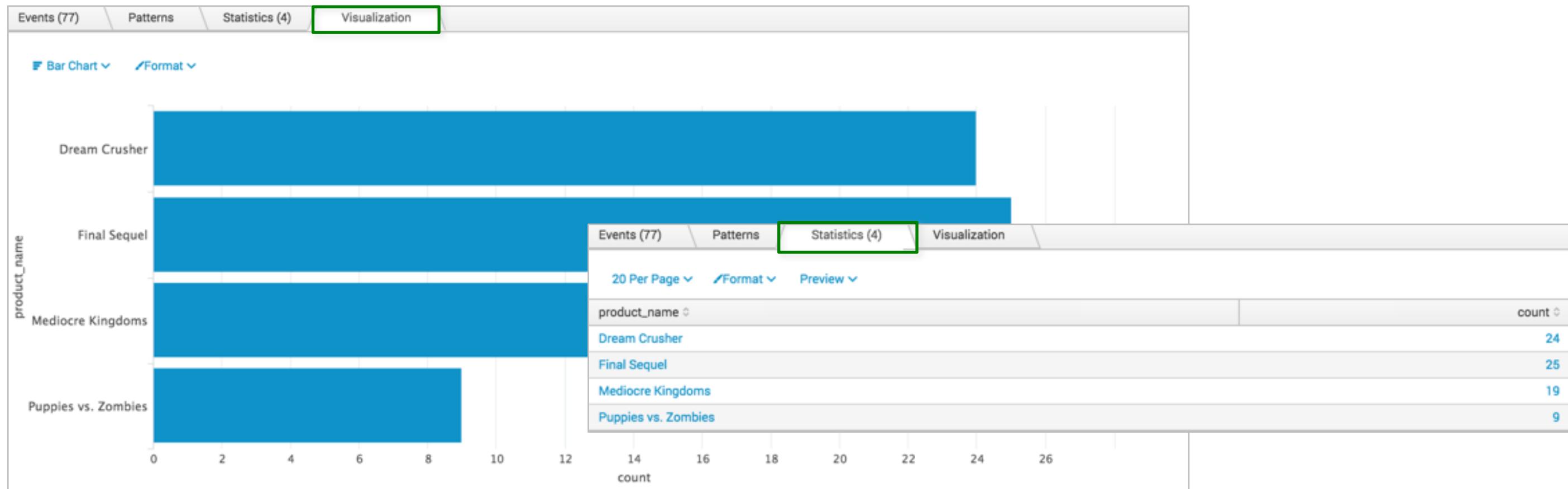
Creating Tables and Visualizations

Three main methods to create tables and visualizations in Splunk are:

- Select a field from the fields sidebar and choose a report to run
- Use the Pivot interface
 - Start with a dataset
or
- Start with Instant Pivot
- Use the Splunk search language transforming commands in the Search bar
 - Transforming commands are discussed in the *Searching & Reporting with Splunk* course

Tables and Visualizations

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

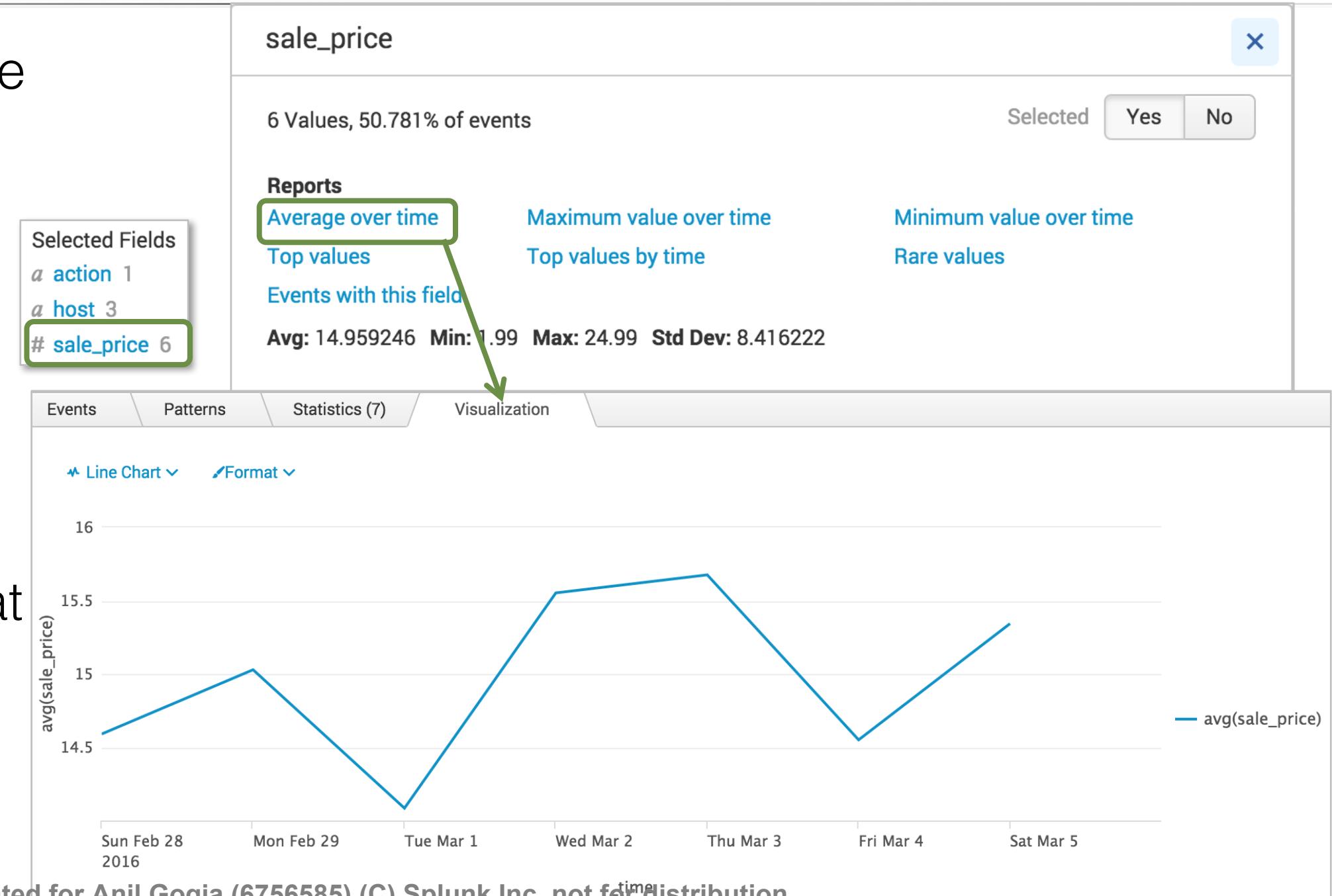


Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Create Reports From the Field Window

- Numeric fields: choose from six report types with mathematical functions, such as average, maximum value, and minimum value

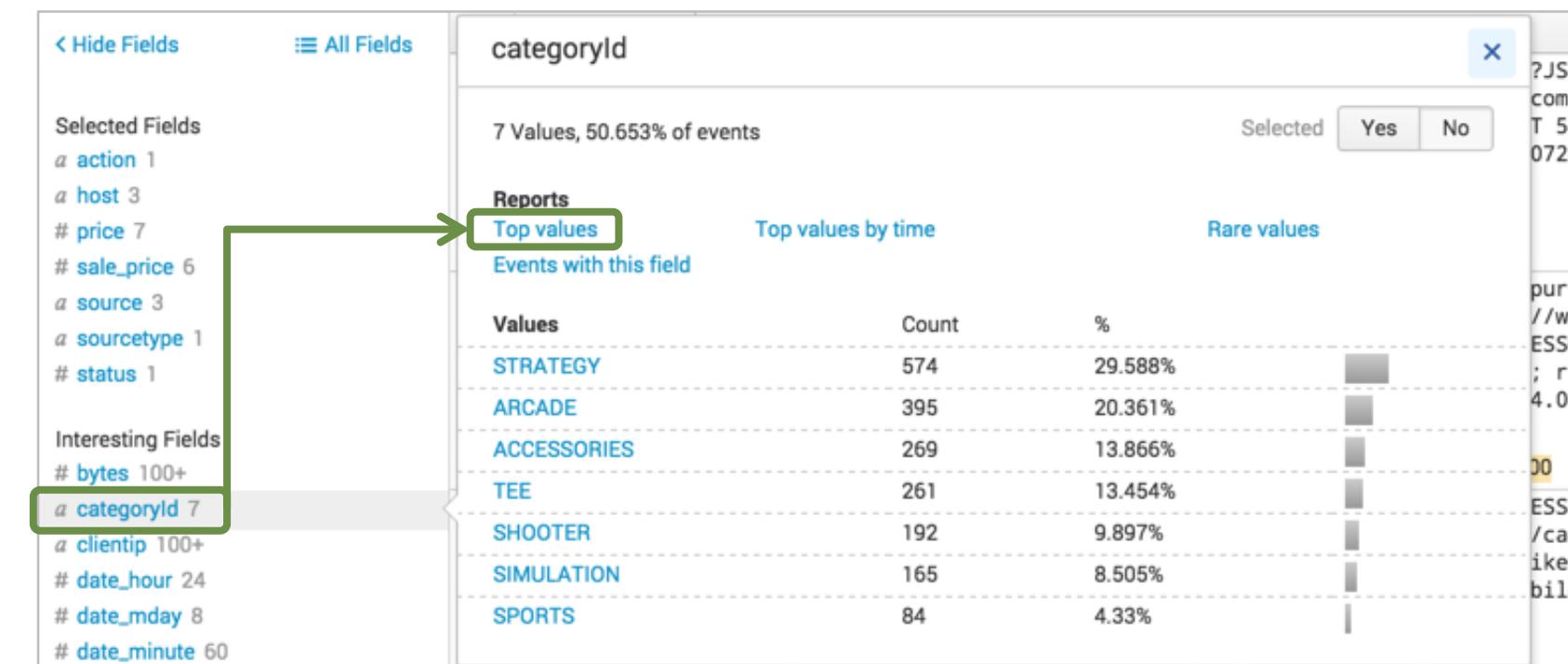
- This example generates a report that shows the average over time
 - This is known as a **timechart**



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Create a Top Values Report

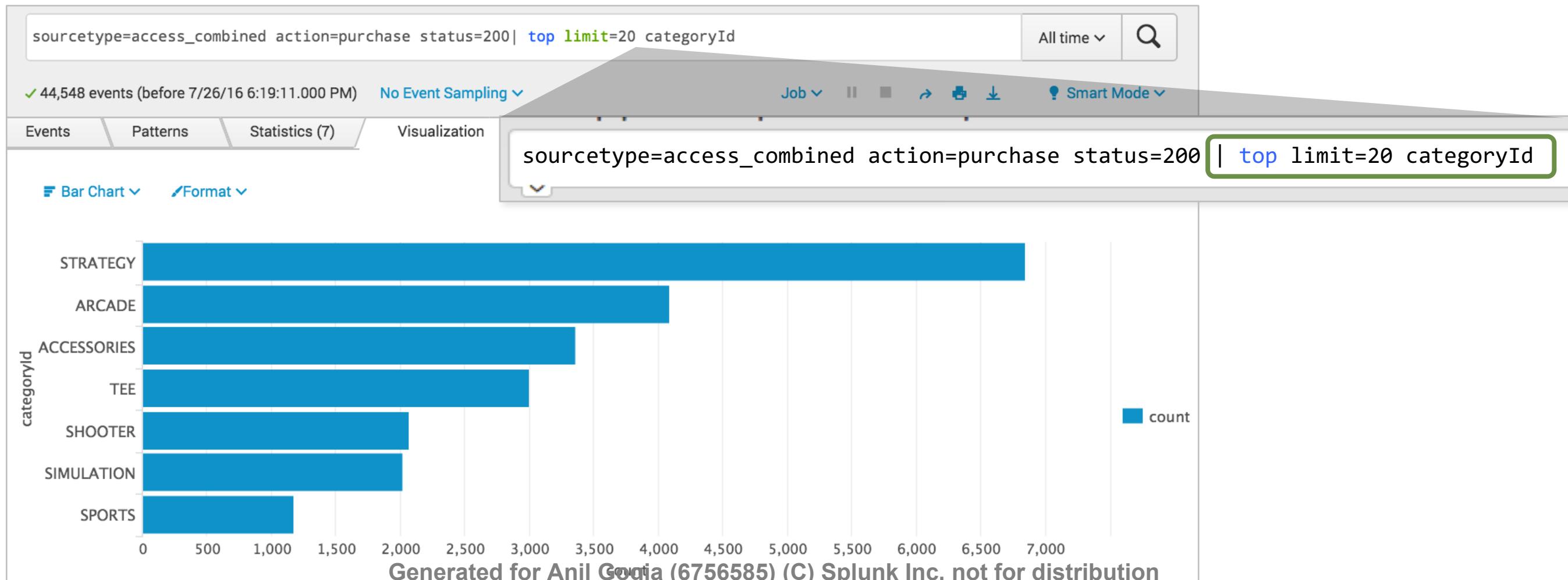
- For alphanumeric character fields, there are only 3 available reports
- In this example, we want a report that shows the top **categories** purchased
 - Basic search: sourcetype=access_combined status=200 action=purchase
 - Click the **categoryId** field
 - Click **Top values**



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

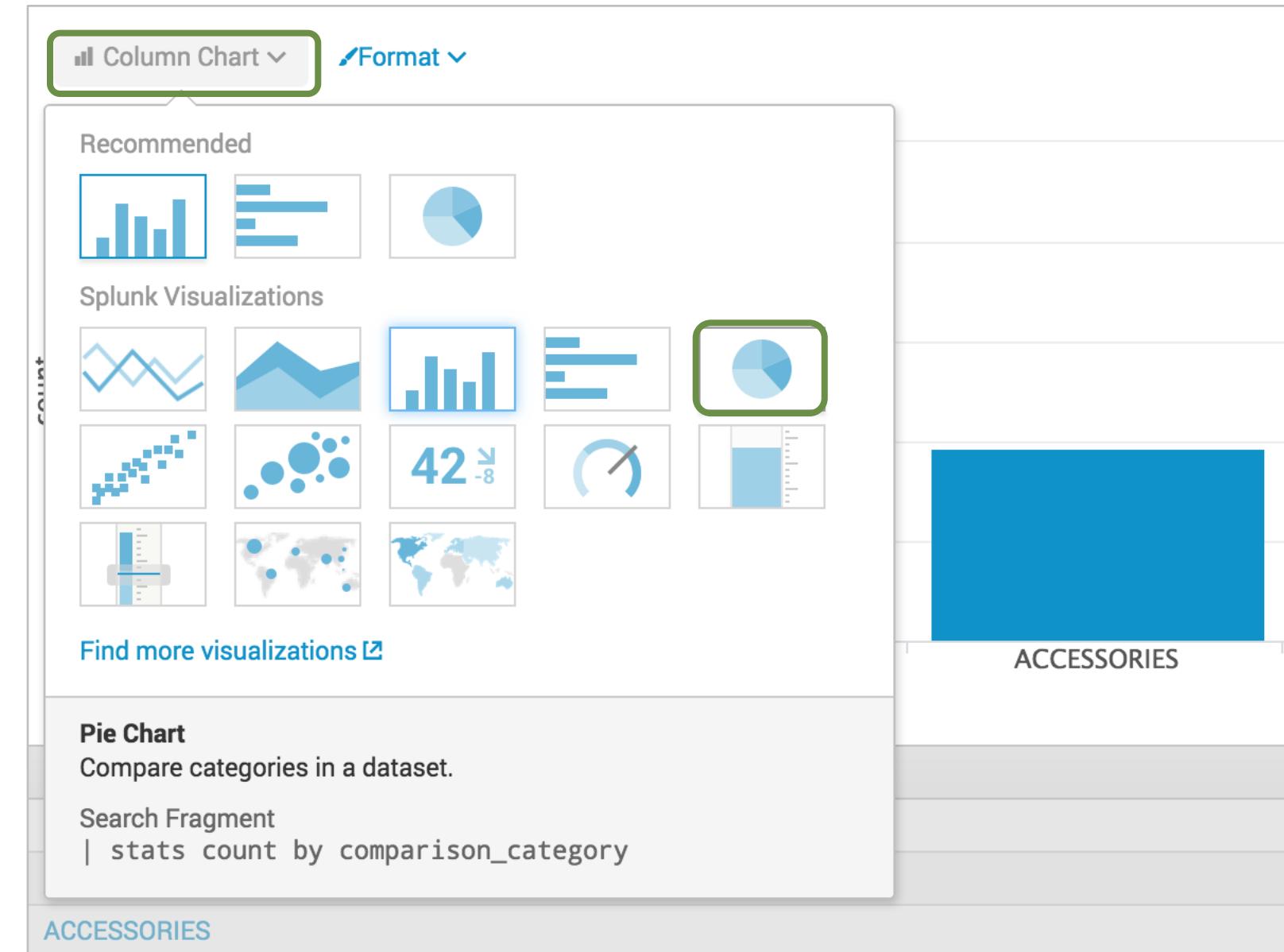
Create a Top Values Report (cont.)

- A | (pipe symbol) and the top command are added to the search string
- A bar chart is returned on the Visualizations tab, displaying the top categories purchased



Change the Visualization

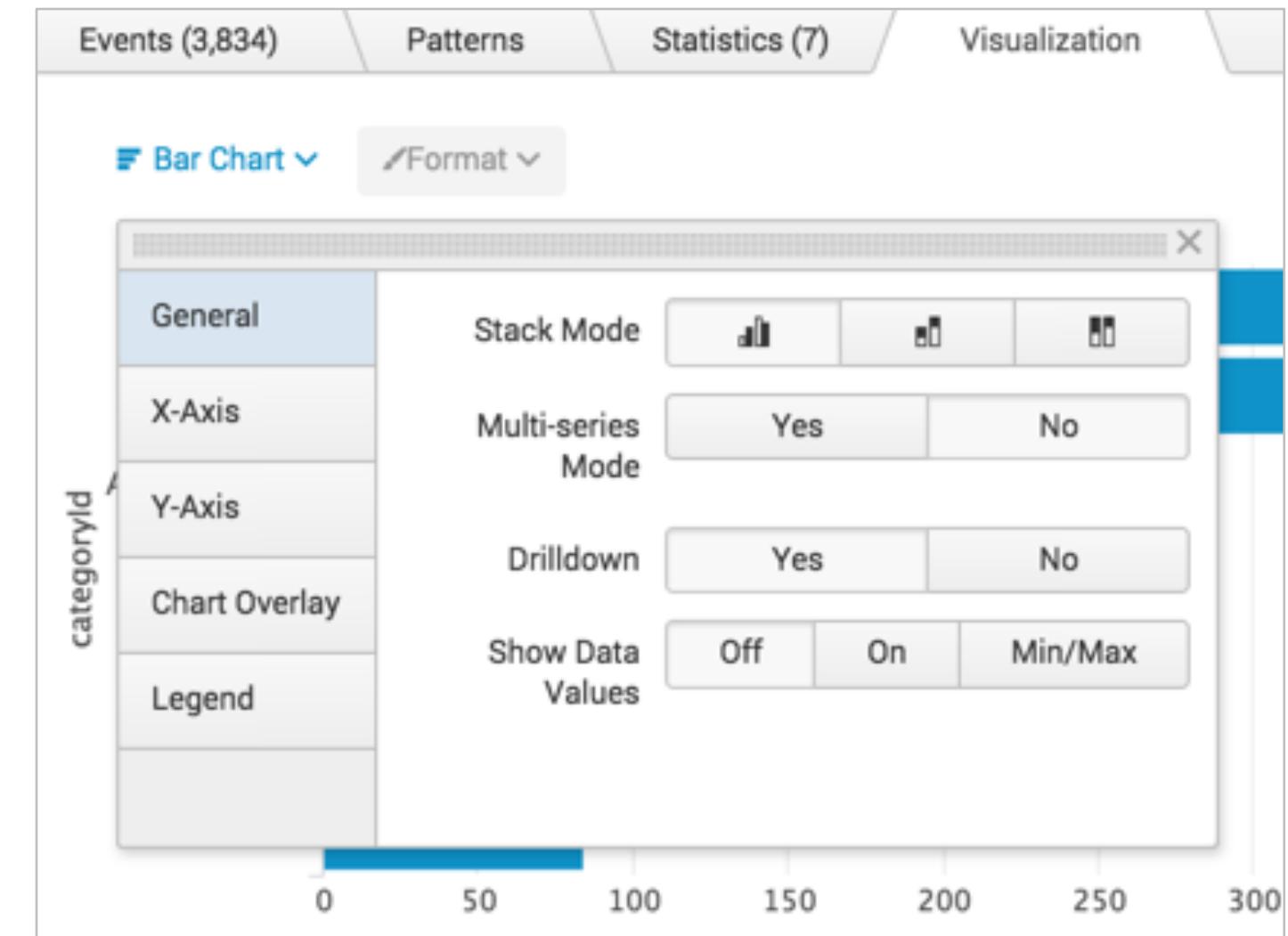
- Select a visualization from the visualization type dropdown menu
- In this example, the column chart is changed to a pie chart



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

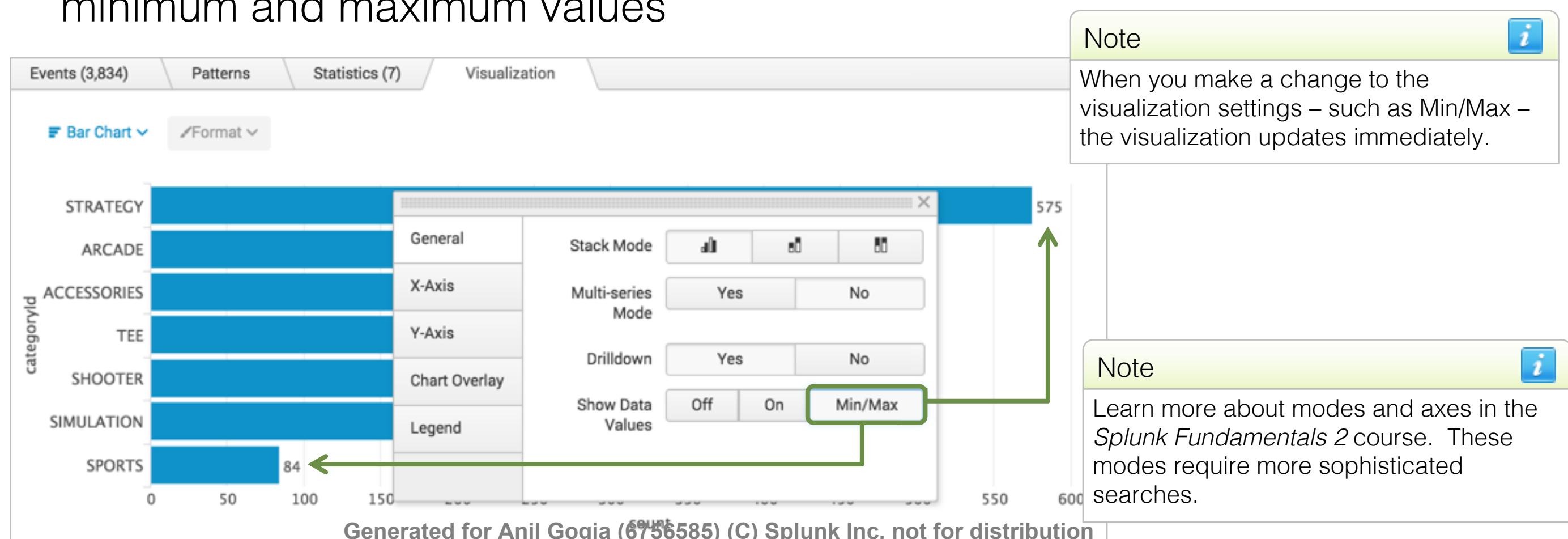
Change the Format

- The **Format** menu allows you to change formatting options
- For example, for bar and column charts:
 - The **General** tab allows you to change Stack, Multi-series, and Drilldown modes
 - The **X-Axis** and **Y-Axis** tabs allow you to change the axis labels and orientation
 - The **Legend** tab allows you to position the visualization legend as desired



Change the Format (cont.)

- **Show Data Values** determines whether to show data values in the visualization
 - If **Min/Max** is selected, data is only shown on the bars containing the minimum and maximum values



View as a Table

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

The screenshot shows a user interface for viewing search results. At the top, there are four tabs: "Events (1,966)", "Patterns", "Statistics (8)", and "Visualization". The "Statistics (8)" tab is currently selected. Below the tabs, there are three dropdown menus: "20 Per Page", "Format", and "Preview". The main area displays a table with the following data:

categoryId	count	percent
STRATEGY	315	23.899848
NULL	246	18.664643
ARCADE	194	14.719272
ACCESSORIES	155	11.760243
TEE	150	11.380880
SIMULATION	103	7.814871
SHOOTER	99	7.511381
SPORTS	56	4.248862

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Statistics Overlay Format

- **Heat map** highlights outstanding values

The screenshot shows the 'Format' dialog box in the Splunk interface, specifically the 'Data Overlay' section. The 'Heat map' option is selected. A green arrow points from the text 'Heat map highlights outstanding values' to this selection. The right side of the screen shows a table with two columns: 'count' and 'percent'. The first row has a red background, indicating it is highlighted by the heat map overlay.

count	percent
6857	30.347422
4092	18.110201
3366	14.897101
3004	13.294977
2071	9.165745
2026	8.966586
1179	5.217969

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

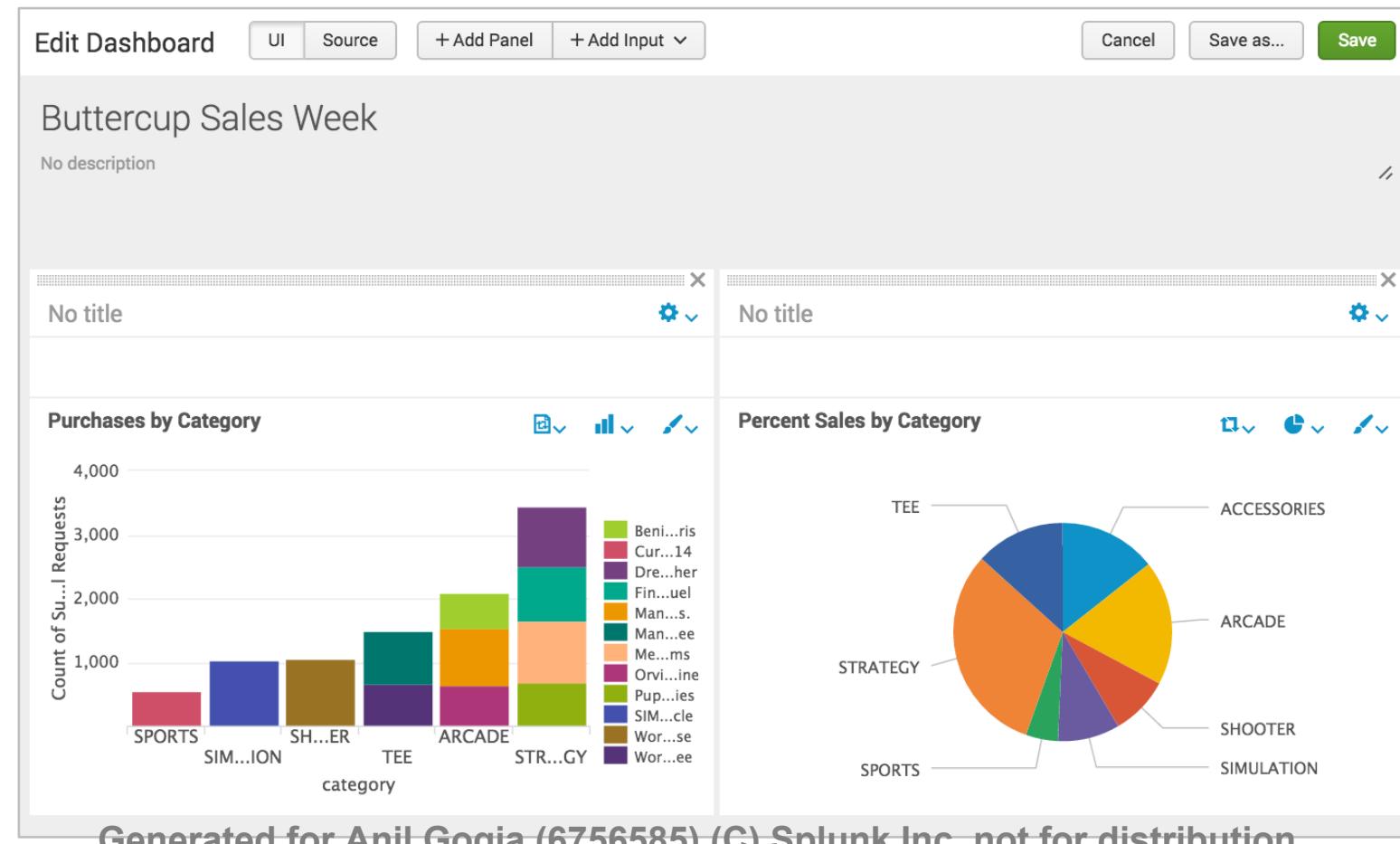
The screenshot shows the 'Format' dialog box in the Splunk interface, specifically the 'Data Overlay' section. The 'High and low values' option is selected. A green arrow points from the text 'High and low values highlights max and min of non zero values' to this selection. The right side of the screen shows a table with two columns: 'count' and 'percent'. The last row has a blue background, indicating it is highlighted by the high/low values overlay.

count	percent
6857	30.347422
4092	18.110201
3366	14.897101
3004	13.294977
2071	9.165745
2026	8.966586
1179	5.217969

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

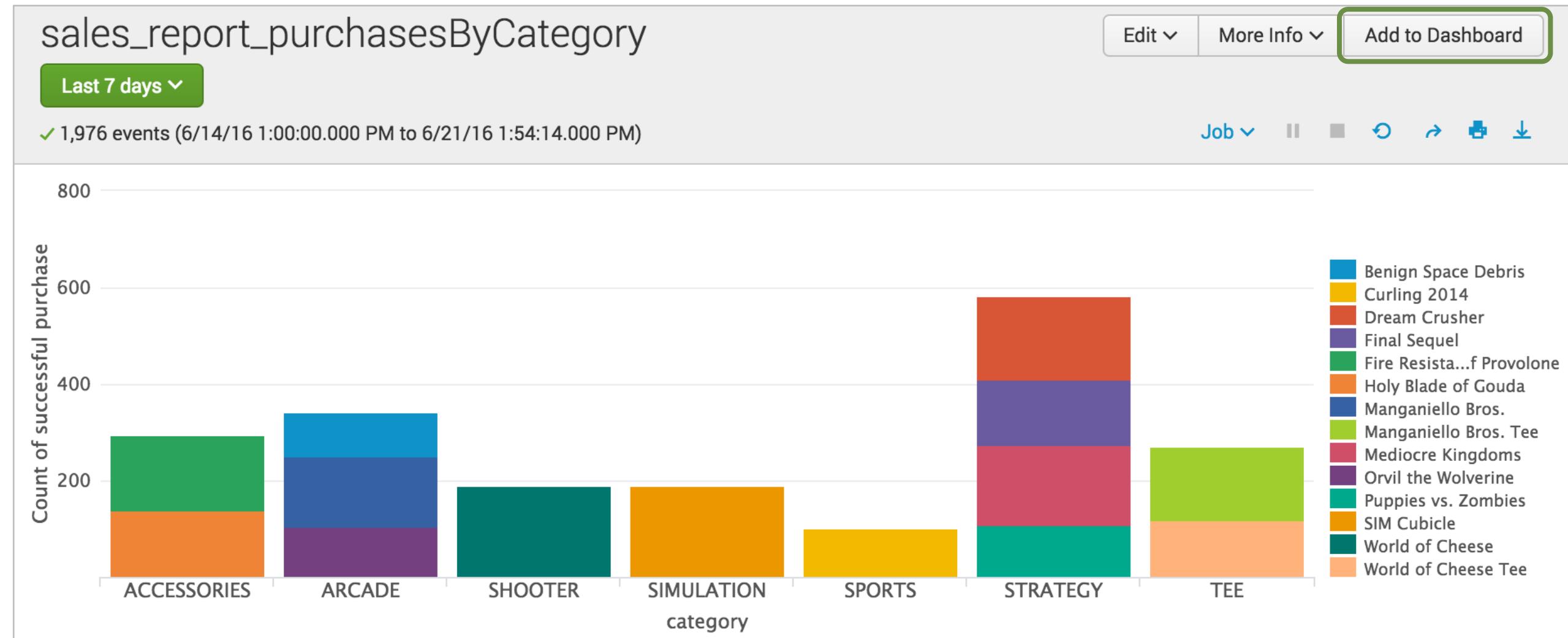
What Is a Dashboard?

- A dashboard consists of one or more panels displaying data visually in a useful way – such as events, tables, or charts
- A report or a pivot can be used to create a panel on a dashboard



Adding a Report to a Dashboard

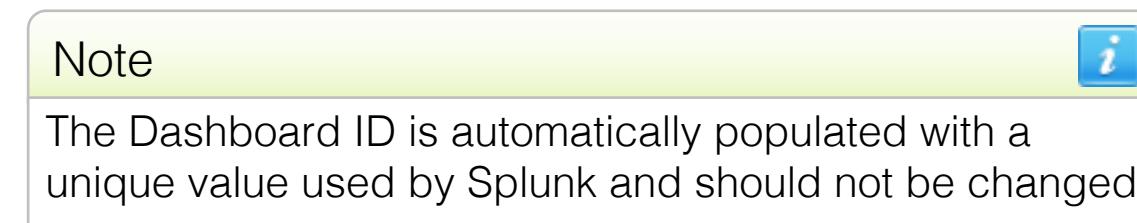
In the report, click **Add to Dashboard** to begin



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Adding a Report to a Dashboard (cont.)

- A Name the dashboard and optionally provide a description
- B Change the permissions (use Private until tested)
- C Enter a meaningful title for the panel
- D For **Panel Powered By**, click **Report**
- E For the **Panel Content**, select **Statistics** to display as a table, or the *visualization type* (in this case, a **Column Chart**)



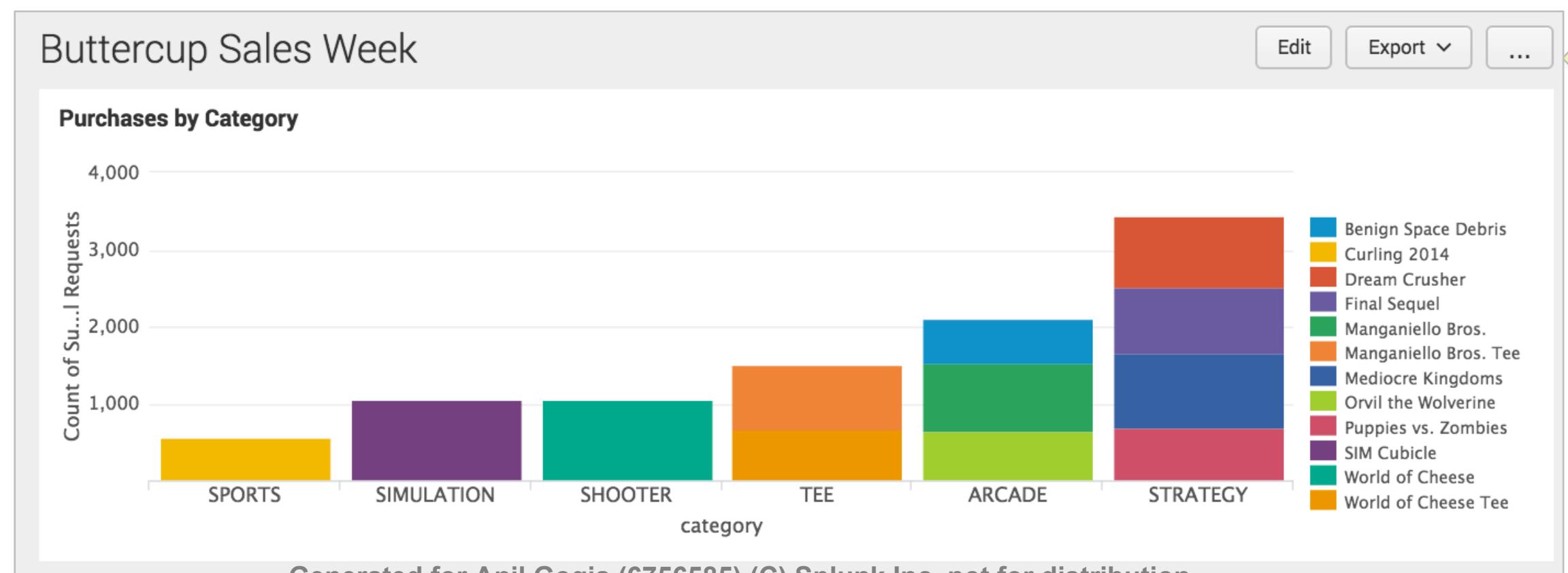
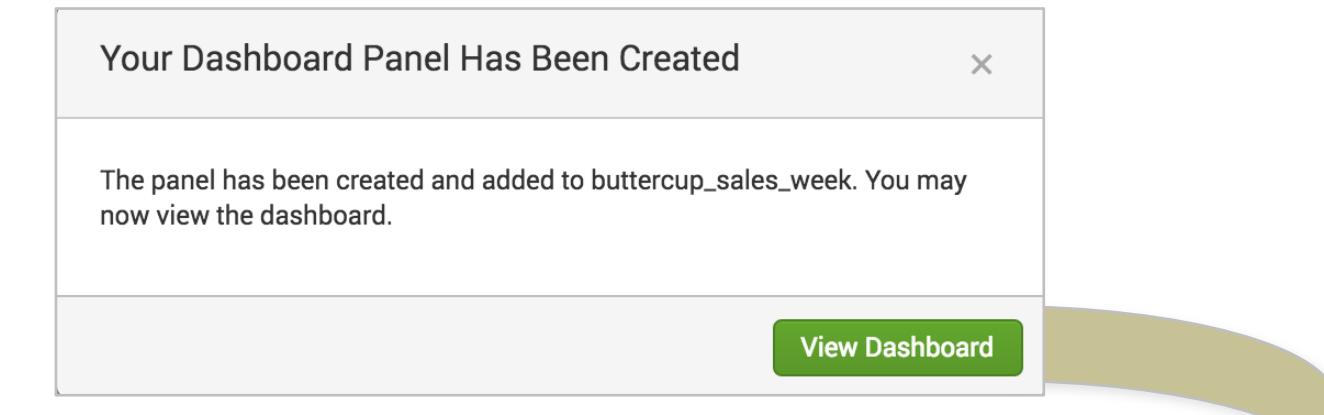
Save As Dashboard Panel

Dashboard	New	Existing
Dashboard Title	Buttercup Sales Week	A
Dashboard ID?	buttercup_sales_week	Can only contain letters, numbers and underscores.
Dashboard Description	optional	
Dashboard Permissions	Private	Shared in App
Panel Title	Purchases by Category	C
Panel Powered By	Inline Search	D Report
Panel Content	Statistics	Column Chart E

Cancel Save

Adding a Report to a Dashboard (cont.)

After it is saved, you can view the dashboard immediately, or select the dashboard from the **Dashboards** view

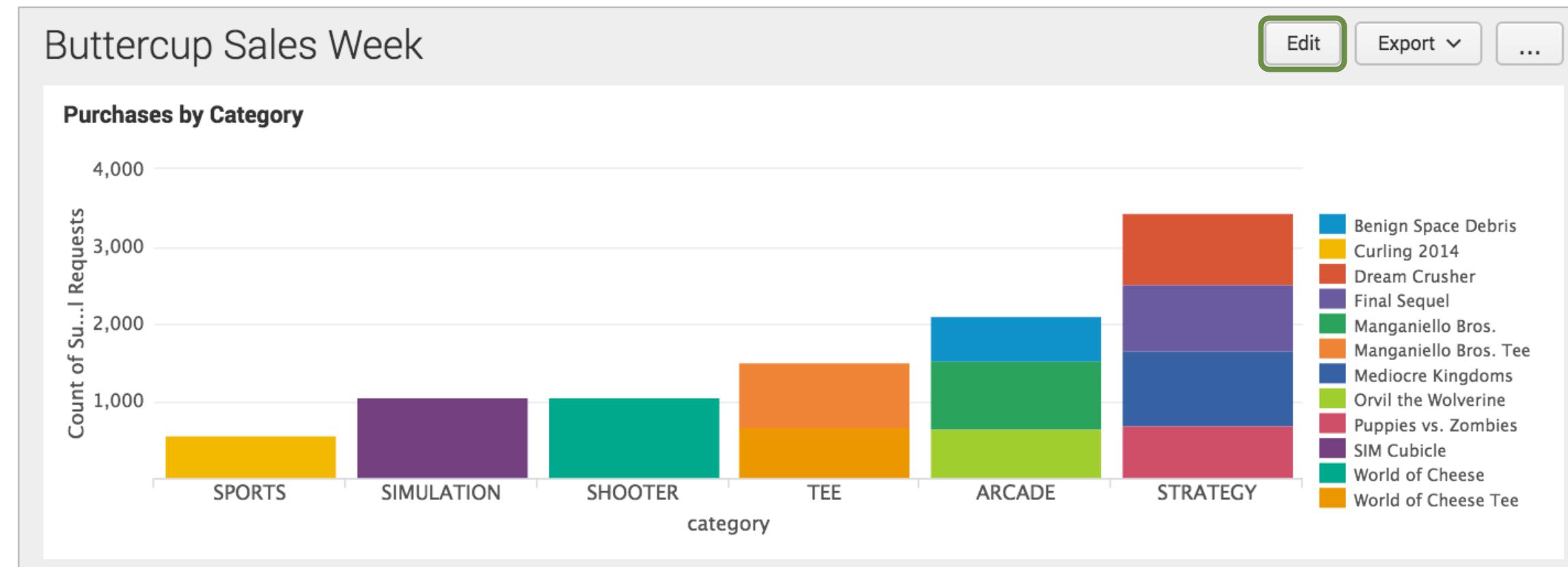


Why Create Panels from Reports?

- It is efficient to create most dashboard panels based on reports because
 - A single report can be used across different dashboards
 - This links the report definition to the dashboard
- Any change to the underlying report will affect every dashboard panel that utilizes that report

Editing Panels

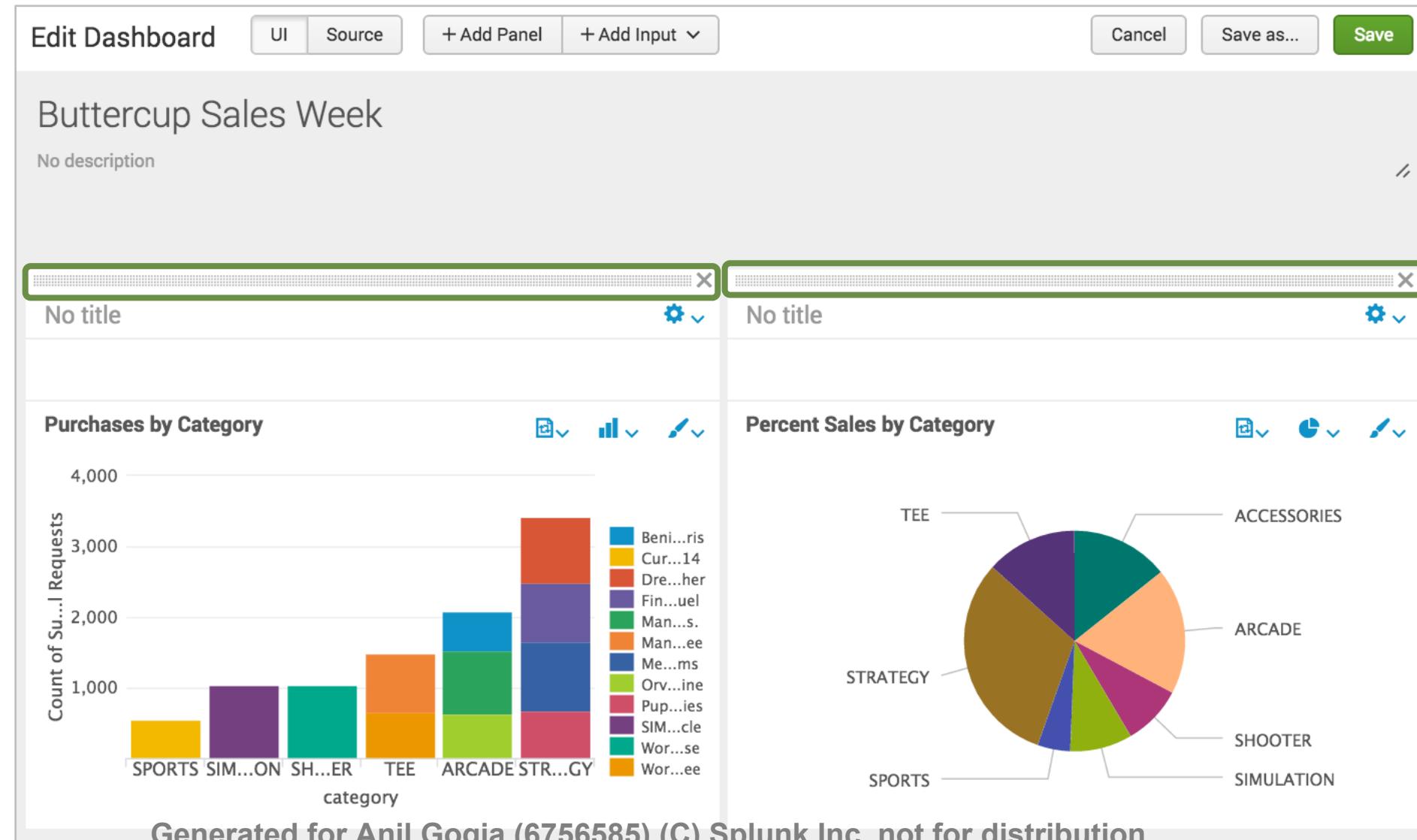
- After saving the panel, a window appears from which you can view the updated dashboard
- Click **Edit** to customize the dashboard



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

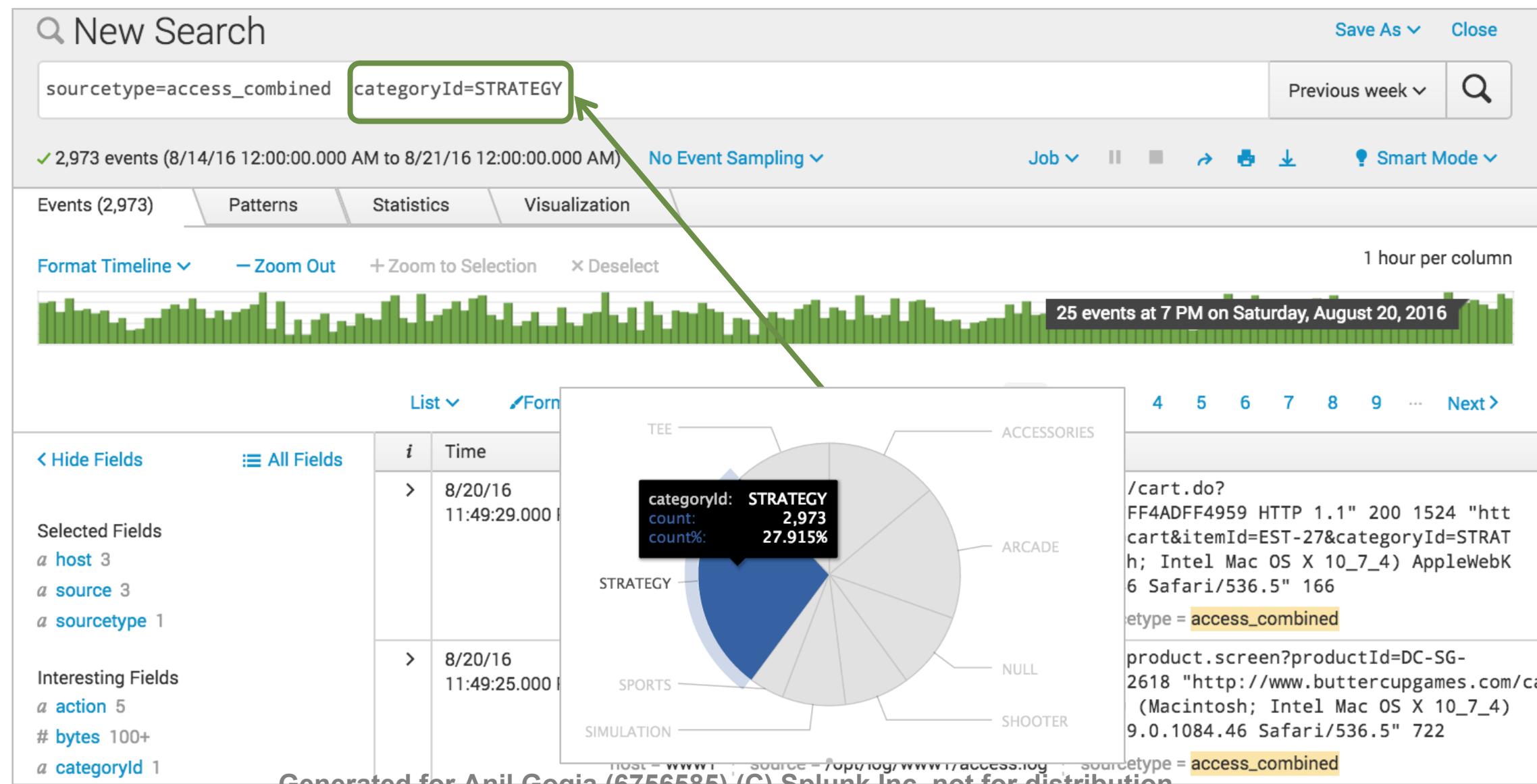
Editing Panel Layout

Click on the dotted bar on a panel to drag the panel to a new location



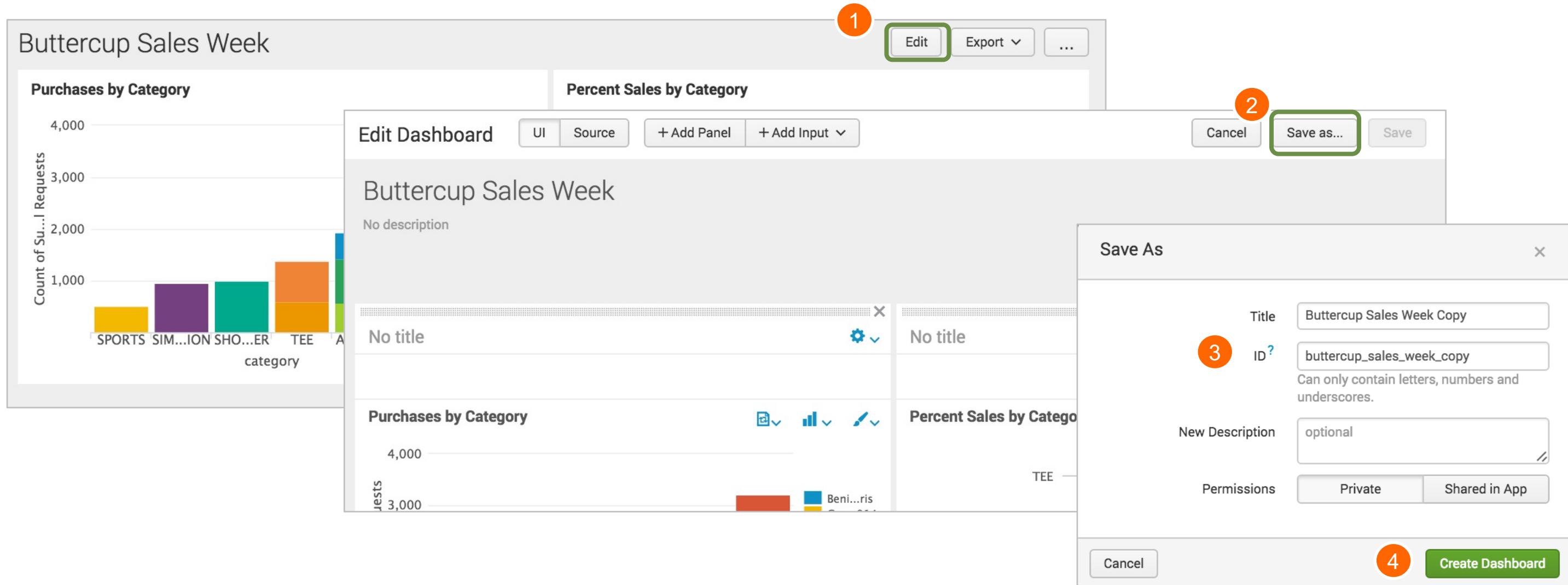
Drill Down from Visualization to Search

Click an object in a chart or table to see its underlying events in Search view



Clone a Dashboard

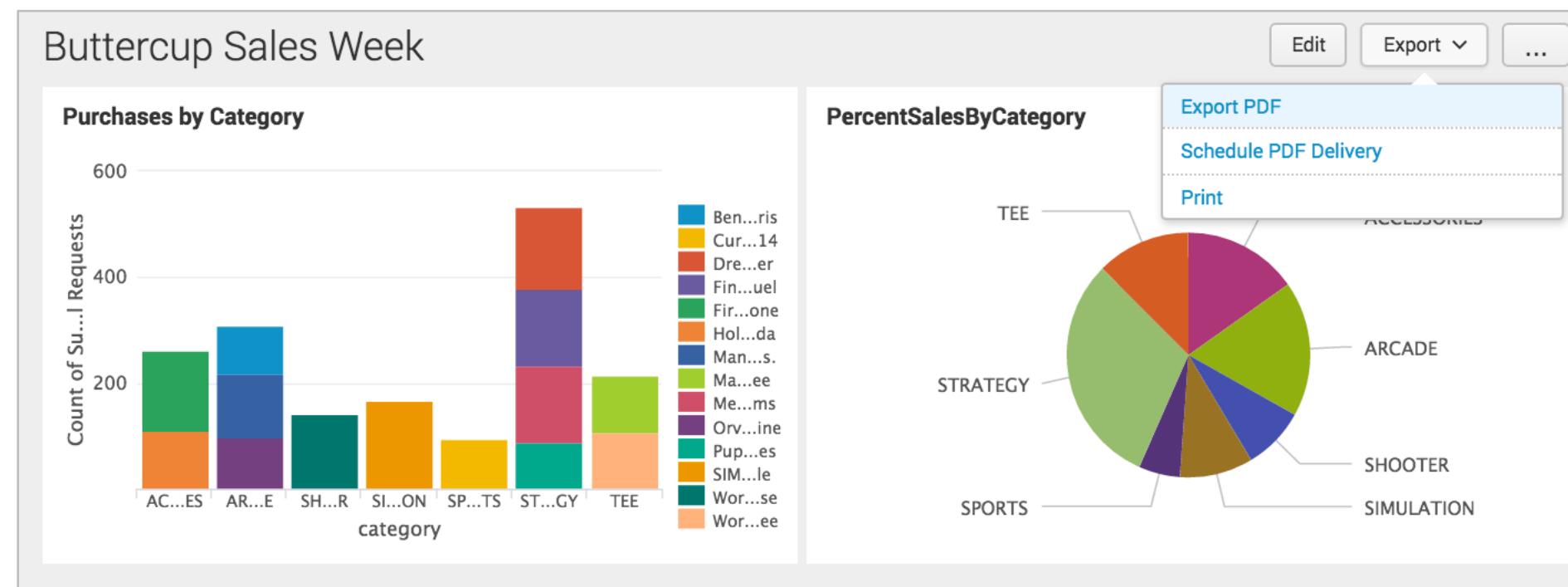
- To clone a dashboard, click **Edit** – and then **Save as...**
 - Change the **Title** as desired, and then click **Create Dashboard**



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Export a Dashboard (cont.)

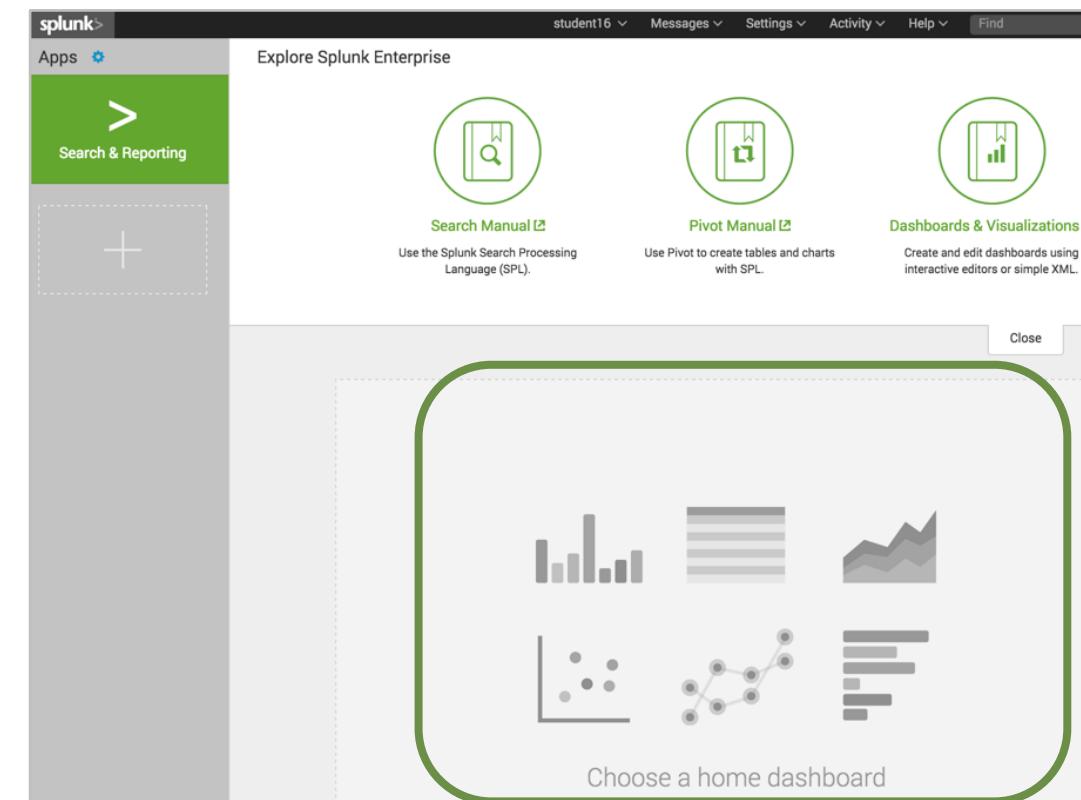
- Without the add-on, dashboards can be exported as PDF
 - They can also be printed



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Make a Default Dashboard

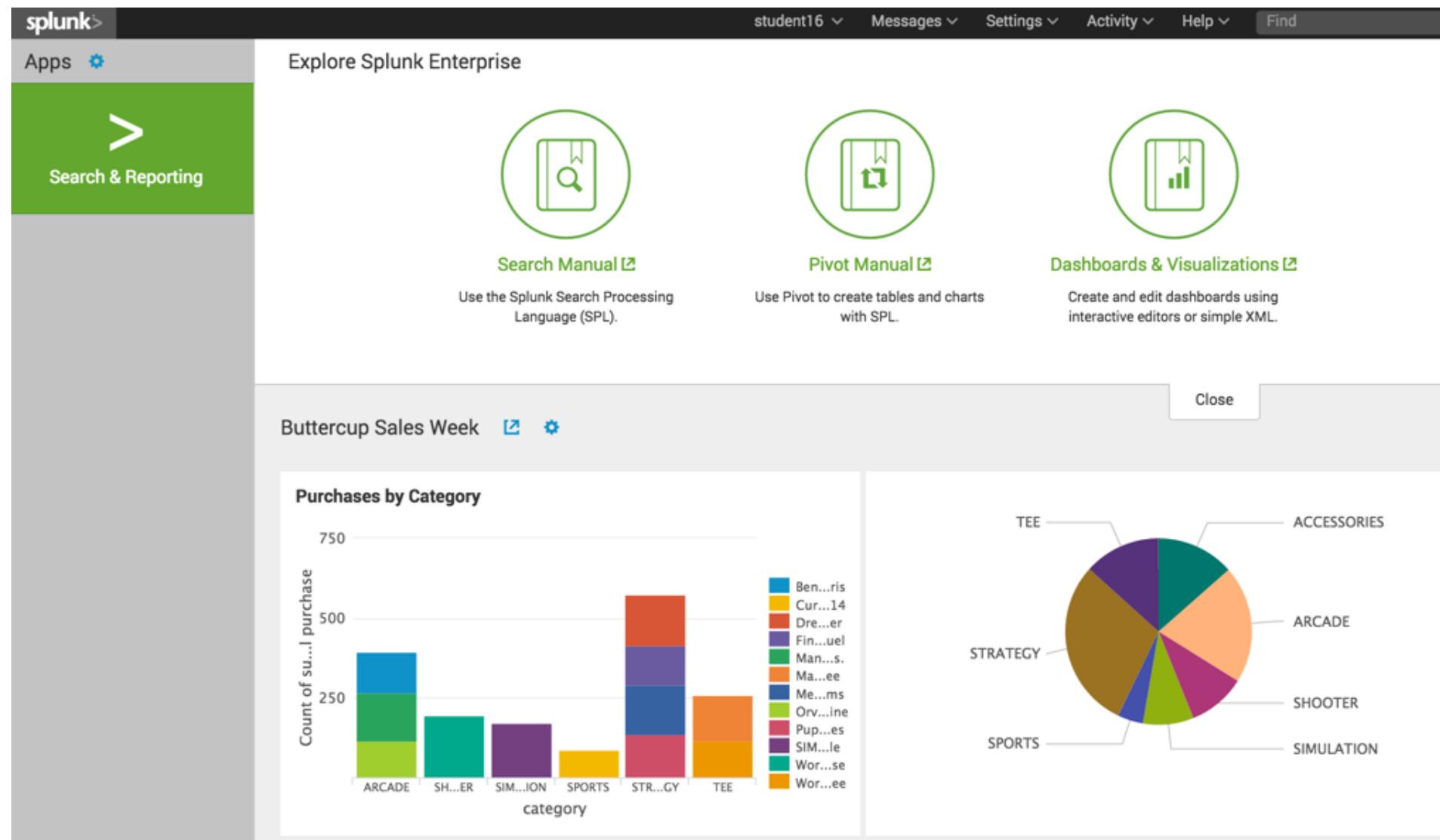
- Set a dashboard to appear by default in the bottom panel of your home view
- From Home, click **Choose a home dashboard**



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

View Your Default Dashboard

After you've set a dashboard as default, your home view may look like this:



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module 11: Using Pivot

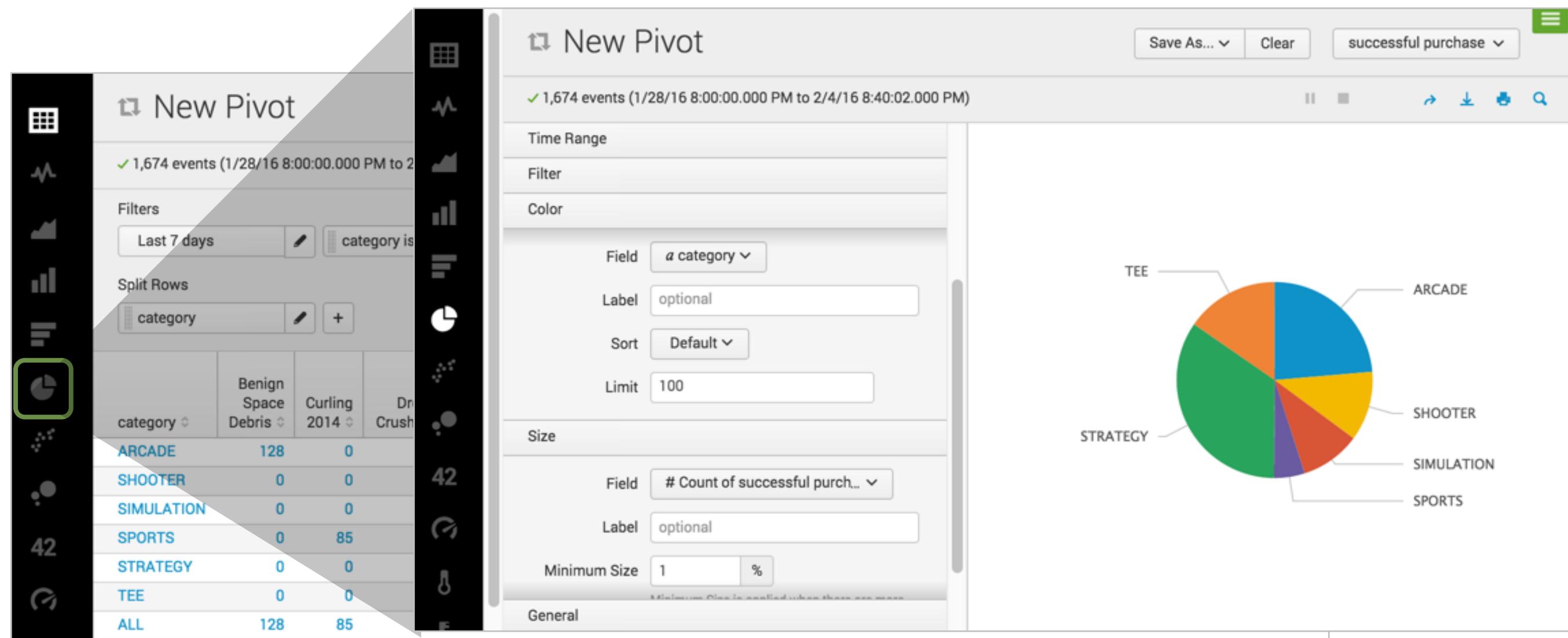
Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

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

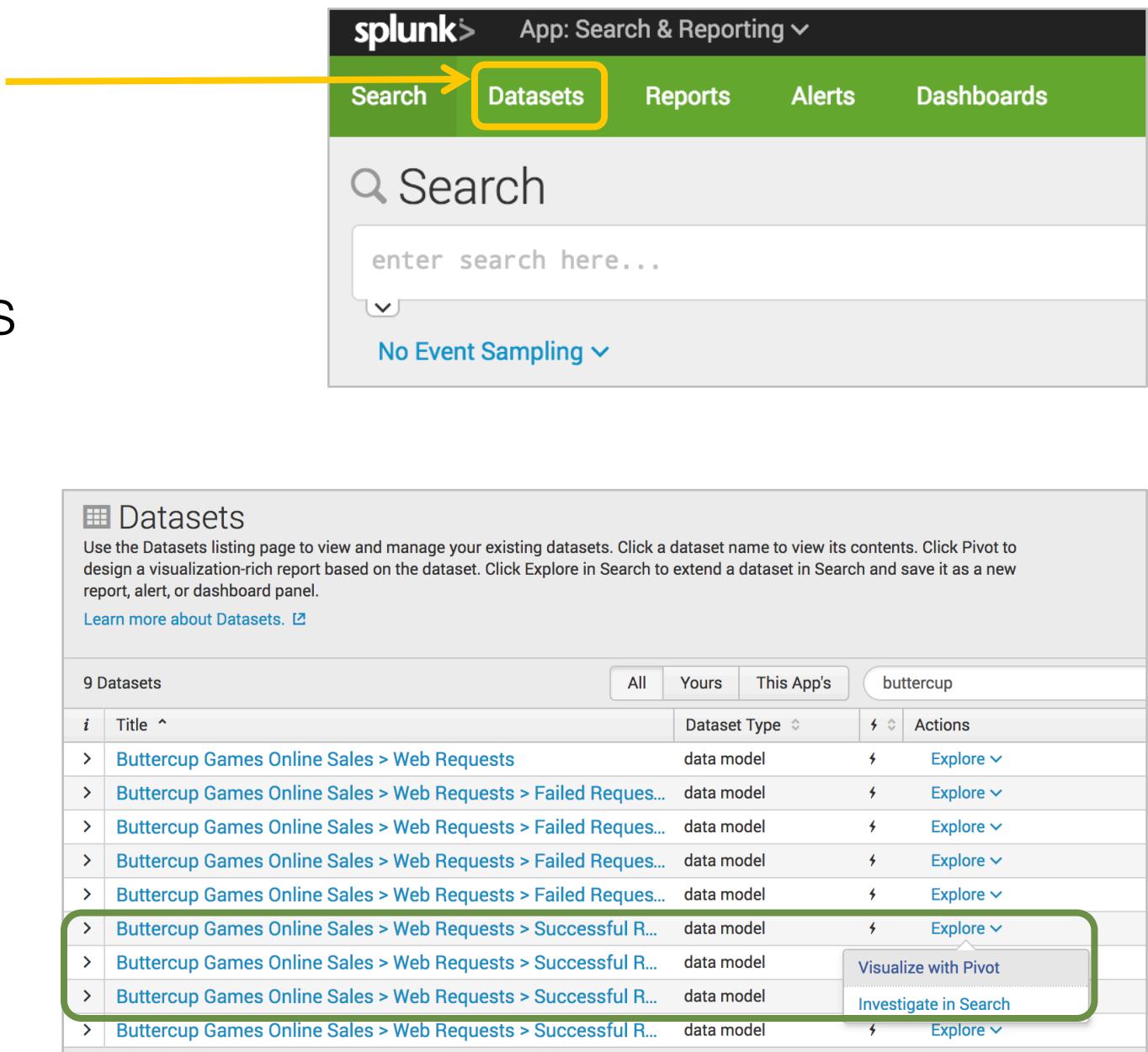
Pivot is a quick way to design visualizations of data. Let's see how.



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Selecting a Dataset

1. From the Search & Reporting app, select the **Datasets** tab
 - This displays a list of available lookup table files ("lookups") and data models
 - Each lookup and data model represent a specific category of data
 - ▶ Prebuilt lookups and data models make it easier to interact with your data
2. Click **Explore > Visualize with Pivot**



The screenshot shows the Splunk interface with the "Datasets" tab highlighted in yellow. The main content area displays a table of datasets with a green rounded rectangle highlighting the last row. A tooltip for this row shows options: "Visualize with Pivot" and "Investigate in Search".

Datasets			
Use the Datasets listing page to view and manage your existing datasets. Click a dataset name to view its contents. Click Pivot to design a visualization-rich report based on the dataset. Click Explore in Search to extend a dataset in Search and save it as a new report, alert, or dashboard panel.			
Learn more about Datasets.			
9 Datasets			
i	Title ^	Dataset Type	Actions
>	Buttercup Games Online Sales > Web Requests	data model	Explore
>	Buttercup Games Online Sales > Web Requests > Failed Reques...	data model	Explore
>	Buttercup Games Online Sales > Web Requests > Failed Reques...	data model	Explore
>	Buttercup Games Online Sales > Web Requests > Failed Reques...	data model	Explore
>	Buttercup Games Online Sales > Web Requests > Failed Reques...	data model	Explore
>	Buttercup Games Online Sales > Web Requests > Successful R...	data model	Explore
>	Buttercup Games Online Sales > Web Requests > Successful R...	data model	Visualize with Pivot Investigate in Search
>	Buttercup Games Online Sales > Web Requests > Successful R...	data model	Explore
>	Buttercup Games Online Sales > Web Requests > Successful R...	data model	Explore

Open in Pivot

- The Pivot automatically populates with a count of events for the selected object
- In this example, it shows all successful purchase requests for all time

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

- Title:** New Pivot
- Event Count:** 208,243 events (before 7/25/16 8:40:39.000 PM)
- Filters:** All time
- Split Rows:** +
- Column Values:** Count of Successf... (highlighted with a green box)
- Value:** 208243
- Buttons:** Save As..., Clear, Documentation, and others.

Generated for Anil Gogia (6756585) (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, it shows all successful purchase requests for all time

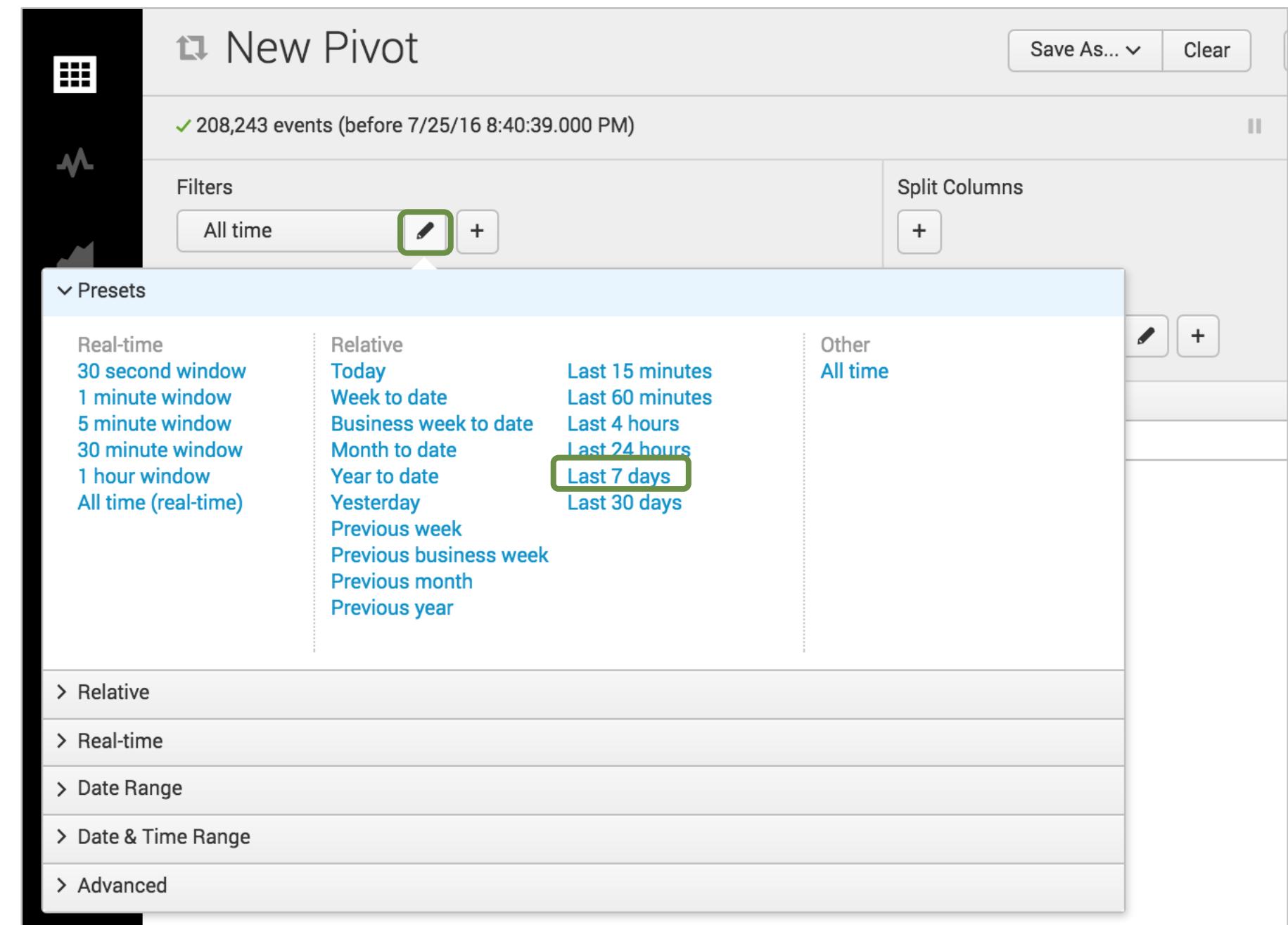
The screenshot shows the Splunk Pivot interface with the following details:

- Title:** New Pivot
- Event Count:** 208,243 events (before 7/25/16 8:40:39.000 PM)
- Filters:** All time
- Split Rows:** +
- Column Values:** Count of Successf... (highlighted with a green box)
- Value:** 208243
- Buttons:** Save As..., Clear, Documentation, and others.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Select a Time Range

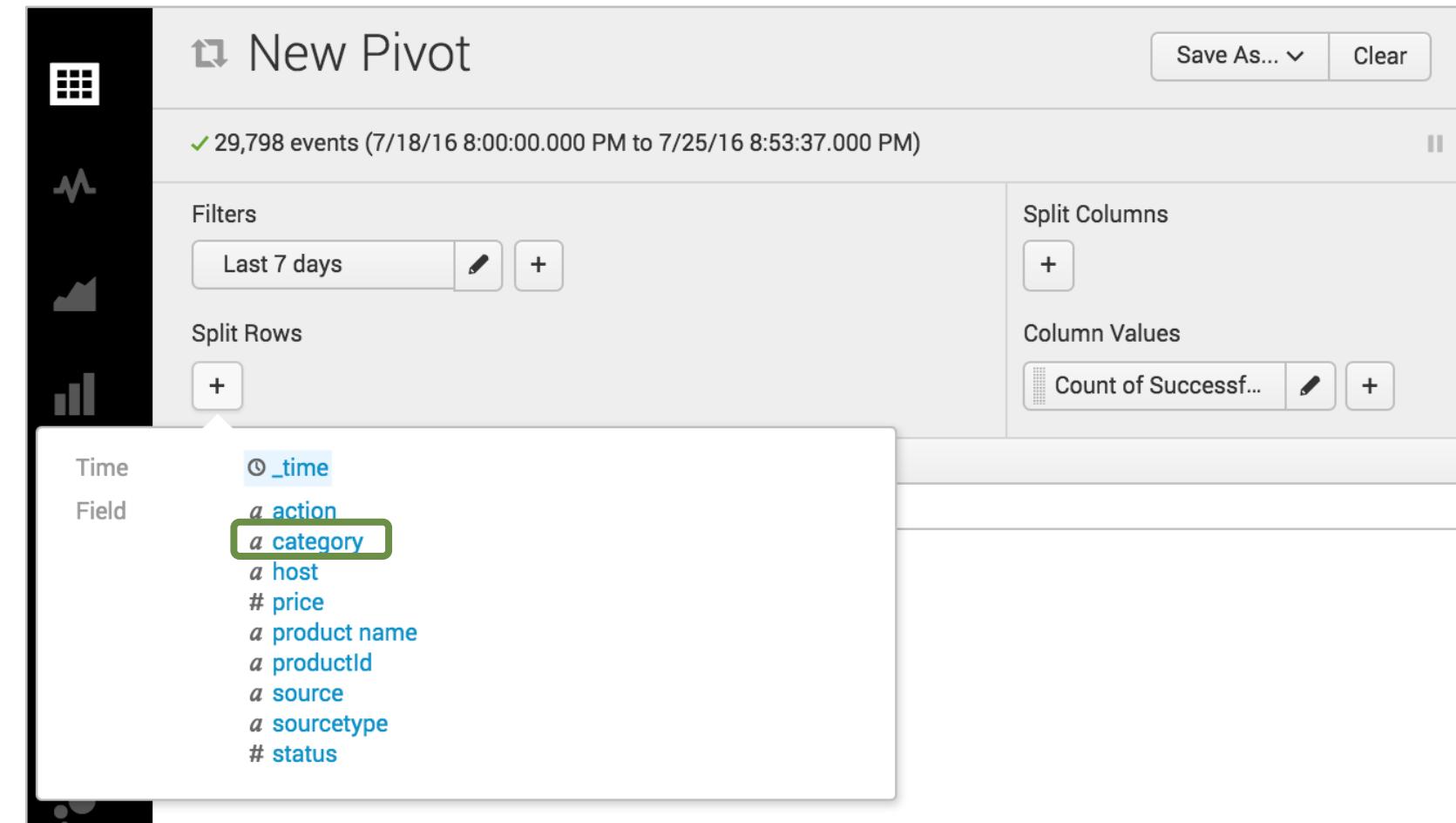
- The default is **All time**
- Click the pencil icon to select the desired time range
- The pivot runs immediately upon selecting the new time range



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Split Rows

- Click  under **Split Rows** for a list of available attributes to populate the rows
- In this example, the rows are split by the **category** attribute, which will list
 - Each game category on a separate row
 - A count of successful requests for each game category

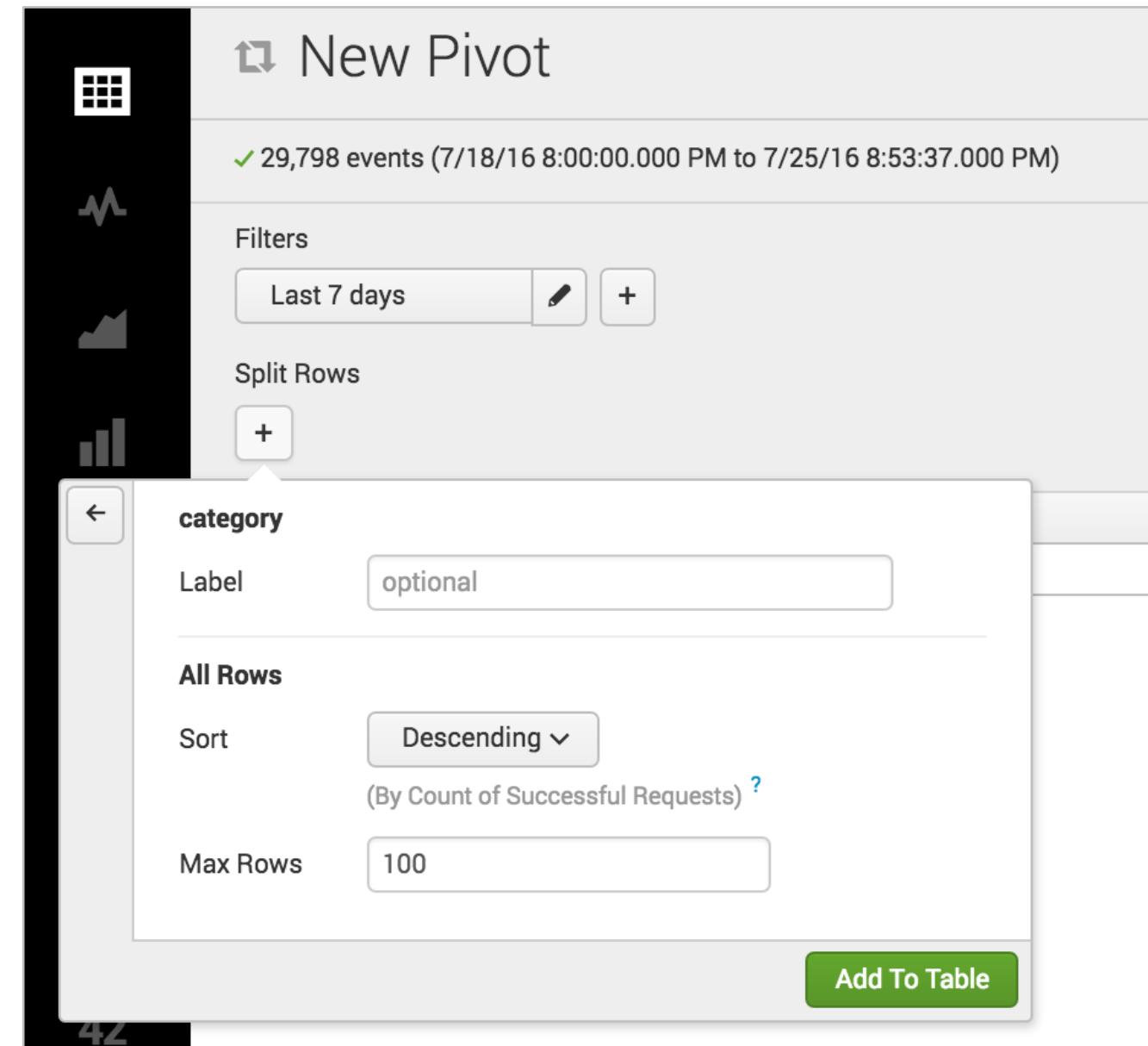


The screenshot shows the Splunk Pivot interface with a modal window titled "Split Rows". The modal lists various attributes under the "Field" section. The "category" attribute is highlighted with a green box. Other listed attributes include _time, action, host, price, product name, product id, source, sourcetype, and status.

Generated for Anil Gogia (6756585) (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
- Click **Add to Table** to view the results



Results

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

- Title:** New Pivot
- Time Range:** 28,021 events (7/19/16 2:00:00.000 PM to 7/26/16 2:58:00.000 PM)
- Filters:** Last 7 days
- Split Rows:** category
- Column Values:** Count of Successf...
- Table Data:**

category	Count of Successful Requests
SPORTS	569
SIMULATION	1053
SHOOTER	1065
TEE	1538
ACCESSORIES	1687
ARCADE	2132
STRATEGY	3482

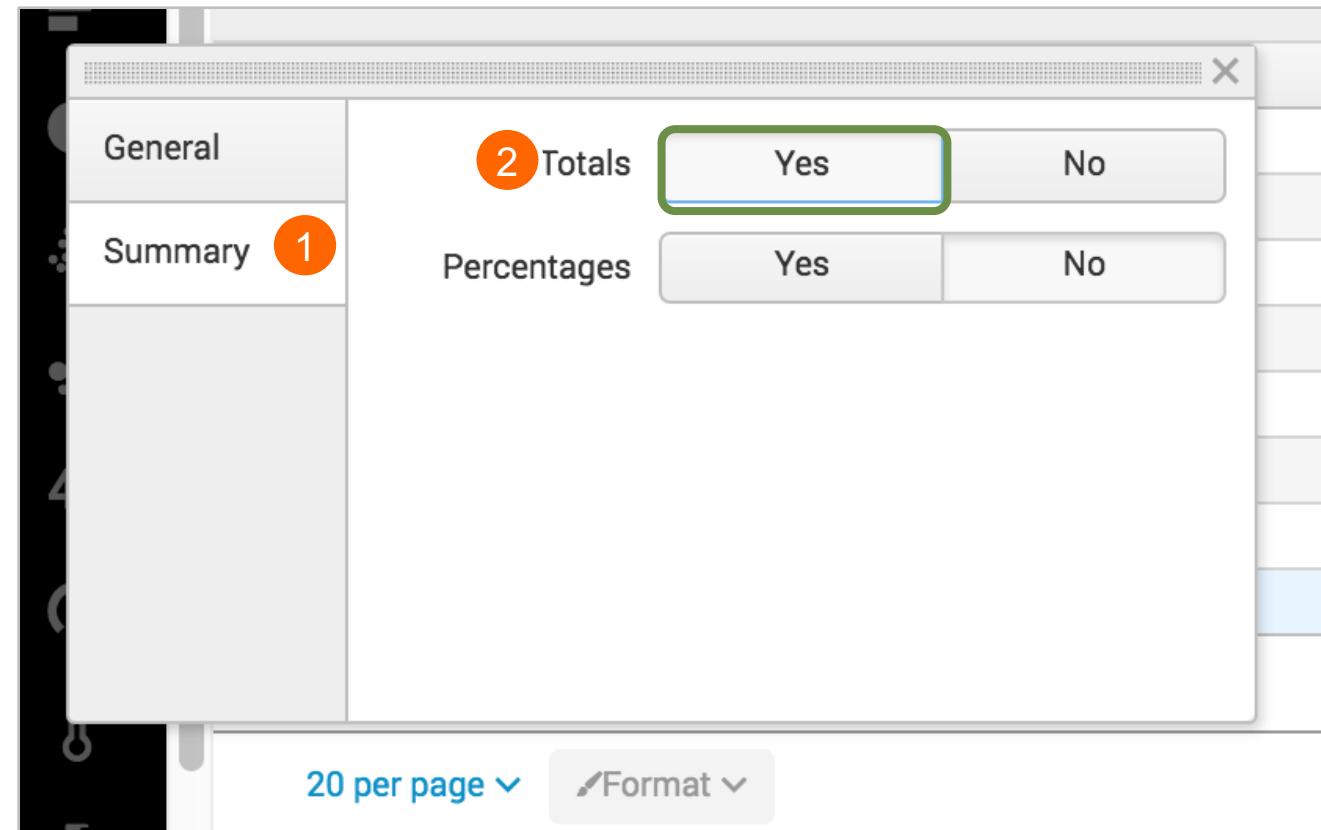
Annotations:

- A yellow callout box labeled "categories" points to the "category" field in the Split Rows section.
- A yellow callout box labeled "count by category" points to the "Count of Successf..." field in the Column Values section.
- A green arrow points from the "Format" button in the bottom navigation bar to a callout box containing the text "To format the results, click here".

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Formatting the Results

For example, to add totals on the **Summary** tab, click **Yes** next to **Totals**



Updated Results (with Total)

The screenshot shows a Splunk Pivot search interface titled "New Pivot". The sidebar on the left contains icons for various search types: Grid, Line, Area, Bar, Histogram, Scatter, Dot, and a value "42". The main pane displays a pivot table with the following data:

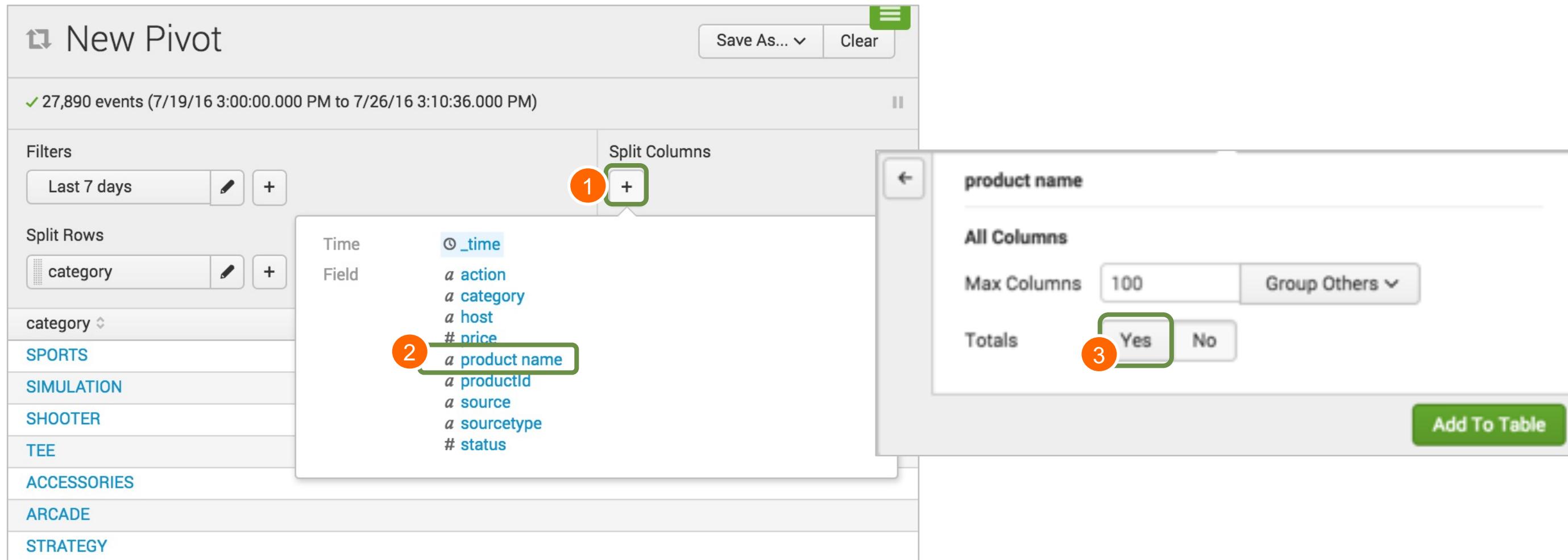
category	Count of Successful Requests
SPORTS	568
SIMULATION	1049
SHOOTER	1059
TEE	1530
ACCESSORIES	1679
ARCADE	2126
STRATEGY	3469
	11480

At the bottom of the table, there is a green arrow pointing to the total value "11480", which is highlighted with a green rounded rectangle. The interface also includes filters for "Last 7 days" and "category", and a column value "Count of Successf...".

Generated for Anil Gogia (6756585) (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



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

- New Pivot**: The title of the search.
- 27,890 events (7/19/16 3:00:00.000 PM to 7/26/16 3:10:36.000 PM)**: The event count and time range.
- Filters**: A section containing:
 - Last 7 days
 - Split Rows
 - category
 - category: SPORTS, SIMULATION, SHOOTER, TEE, ACCESSORIES, ARCADE, STRATEGY
- Split Columns**: A button with a green plus sign, circled with orange number 1.
- Time**: A dropdown menu showing @_time.
- Field**: A dropdown menu showing:
 - a action
 - a category
 - a host
 - # price
 - a product name
 - a productId
 - a source
 - a sourcetype
 - # statusItem "a product name" is highlighted with a green box and circled with orange number 2.
- product name**: A field entry in the Split Columns dialog.
- All Columns**: A section in the Split Columns dialog.
- Max Columns**: A text input set to 100, with a "Group Others" dropdown.
- Totals**: A section in the Split Columns dialog with "Yes" (circled with orange number 3) and "No" buttons.
- Add To Table**: A green button at the bottom right of the Split Columns dialog.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Results

New Pivot

Save As... Clear Successful Requests

✓ 27,880 events (7/19/16 4:00:00.000 PM to 7/26/16 4:52:58.000 PM)

Filters: Last 7 days, +

Split Rows: category, +

Split Columns: product name, +

Column Values: Count of Success..., +

The ALL column shows row totals by category

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 Tee	World of Cheese Tee	ALL
SPORTS	0	568	0	0	0	0	0	0	0	0	0	0	0	0	568
SIMULATION	0	0	0	0	0	0	0	0	0	0	0	1055	0	0	1055
SHOOTER	0	0	0	0	0	0	0	0	0	0	0	0	0	1069	0
TEE	0	0	0	0	0	0	0	855	0	0	0	0	0	0	667
ACCESSORIES	0	0	0	0	863	814	0	0	0	0	0	0	0	0	1677
ARCADE	572	0	0	0	0	0	907	0	0	647	0	0	0	0	2126
STRATEGY	0	0	947	853	0	0	0	986	0	675	0	0	0	0	3461
	572	568	947	853	863	814	907	855	986	647	675	1055	1069	667	11478

The bottom (bolded) row shows column totals by product name

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Add Additional Filters

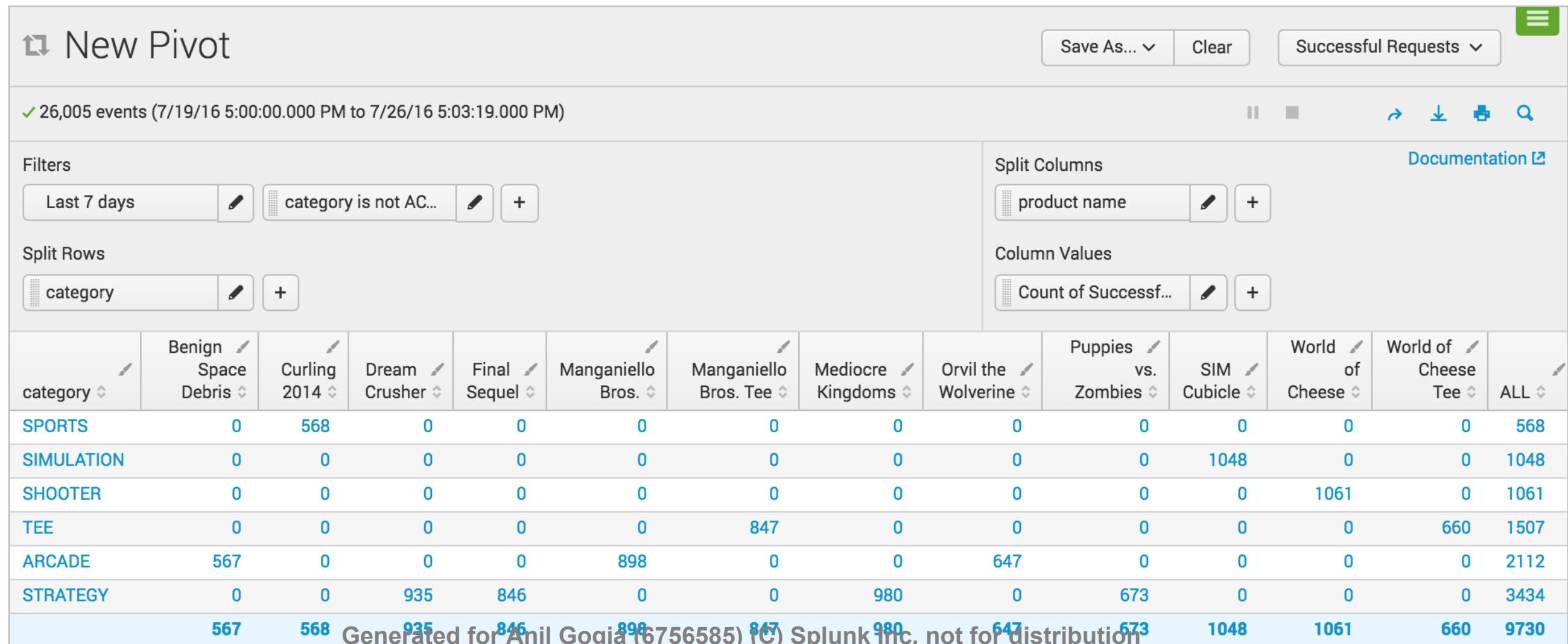
- You can refine a pivot by filtering on key/value pairs
 - Think of ‘split by’ as rows and columns as the fields to display
 - Think of filters as a field=value inclusion, exclusion or specific condition to apply to the search (=, <, >, !=, *)
- In the example, the pivot is filtered to exclude events from the ACCESSORIES category

The screenshot shows two panels of the Splunk 'New Pivot' interface. The left panel displays a list of attributes: action, category, host, price, product name, productId, source, source type, and status. The 'category' attribute is selected and highlighted with a green border. The right panel shows the filter configuration for the 'category' attribute. It includes a 'Filter Type' section with 'Match' and 'Limit' options, and a 'Match' section where the condition 'is not' is selected and the value 'ACCESSORIES' is entered. A dropdown menu next to 'ACCESSORIES' contains the number '5'. At the bottom right of the right panel is a green 'Add To Table' button. Numbered circles (1 through 6) are overlaid on the interface to indicate specific steps: 1 points to the '+' button in the top right of the left panel; 2 points to the 'category' attribute in the list; 3 points to the 'is not' dropdown; 4 points to the 'ACCESSORIES' input field; 5 points to the dropdown menu next to 'ACCESSORIES'; and 6 points to the 'Add To Table' button.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

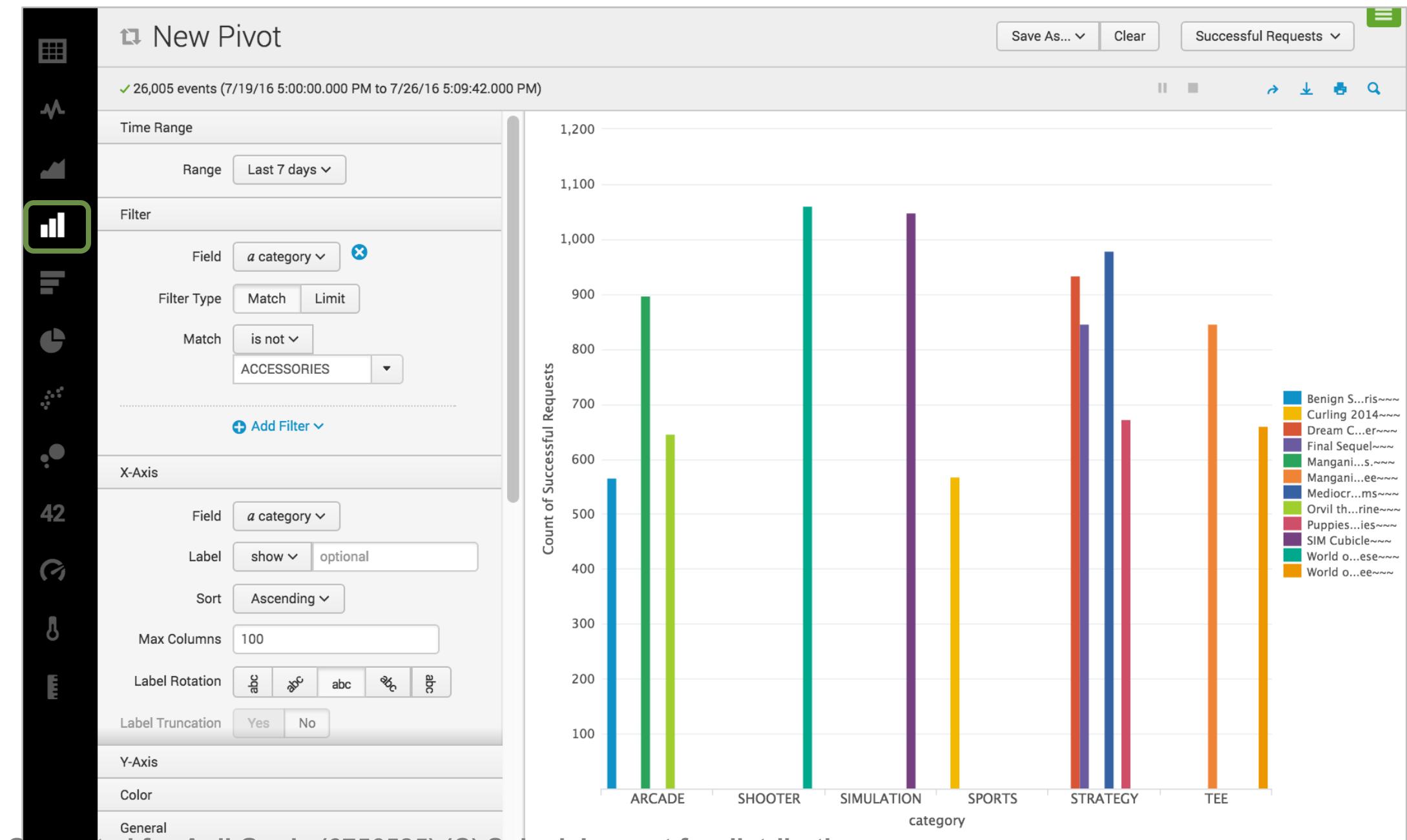
Filtered Pivot

- The ACCESSORIES category is filtered out
- All the other categories remain



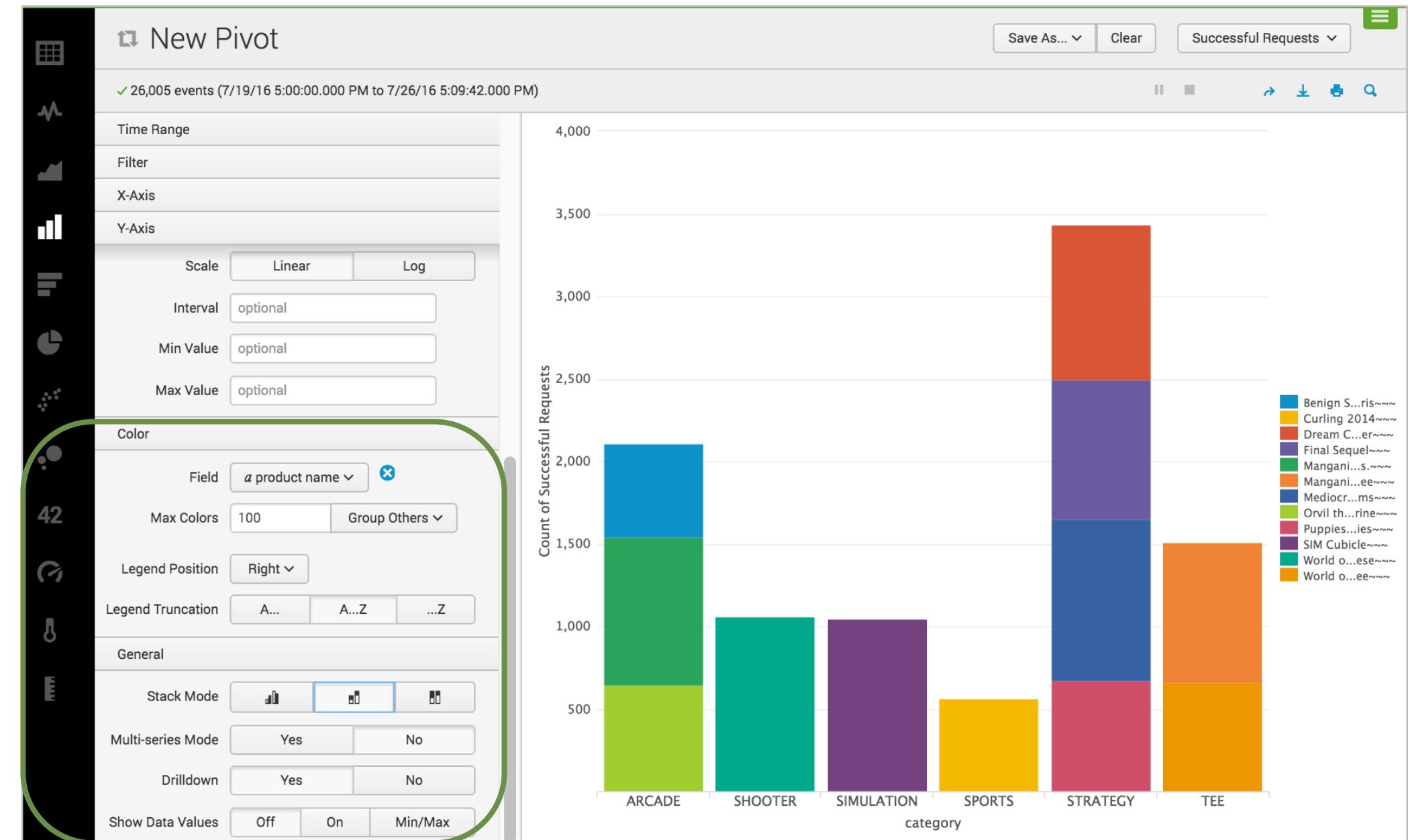
Select a Visualization Format

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



Modify Visualization Settings

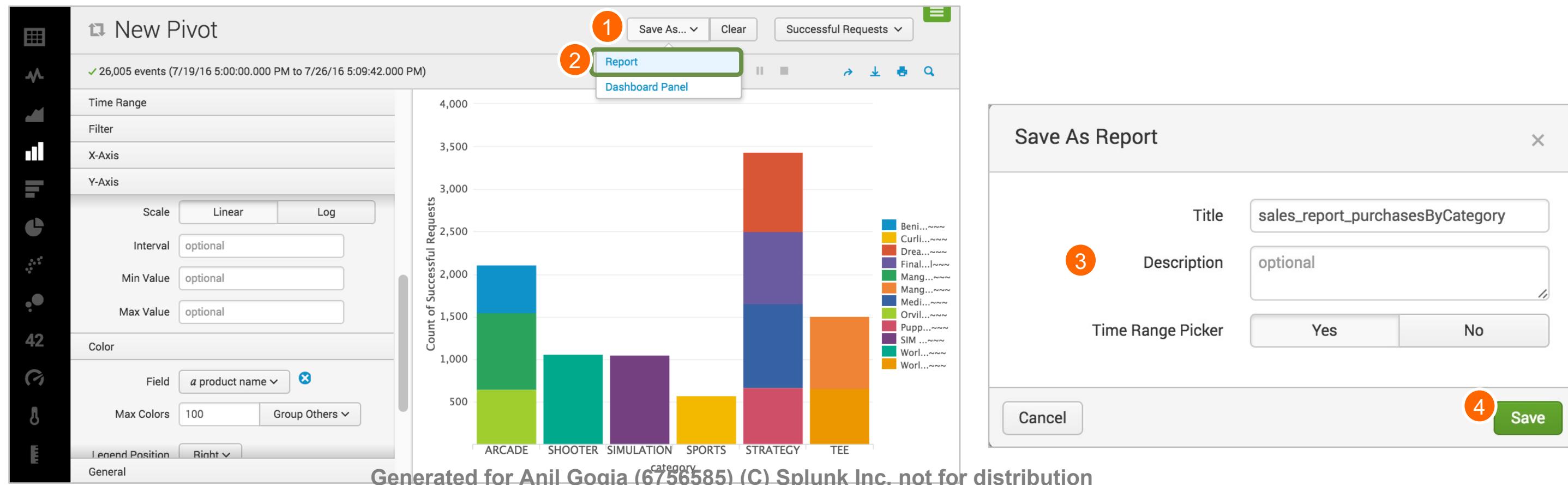
- When a visualization control is selected, panels appear that let you configure its settings
- In this example:
 - The results for each category are broken down by **product_name**
 - The stack mode is set to stacked



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

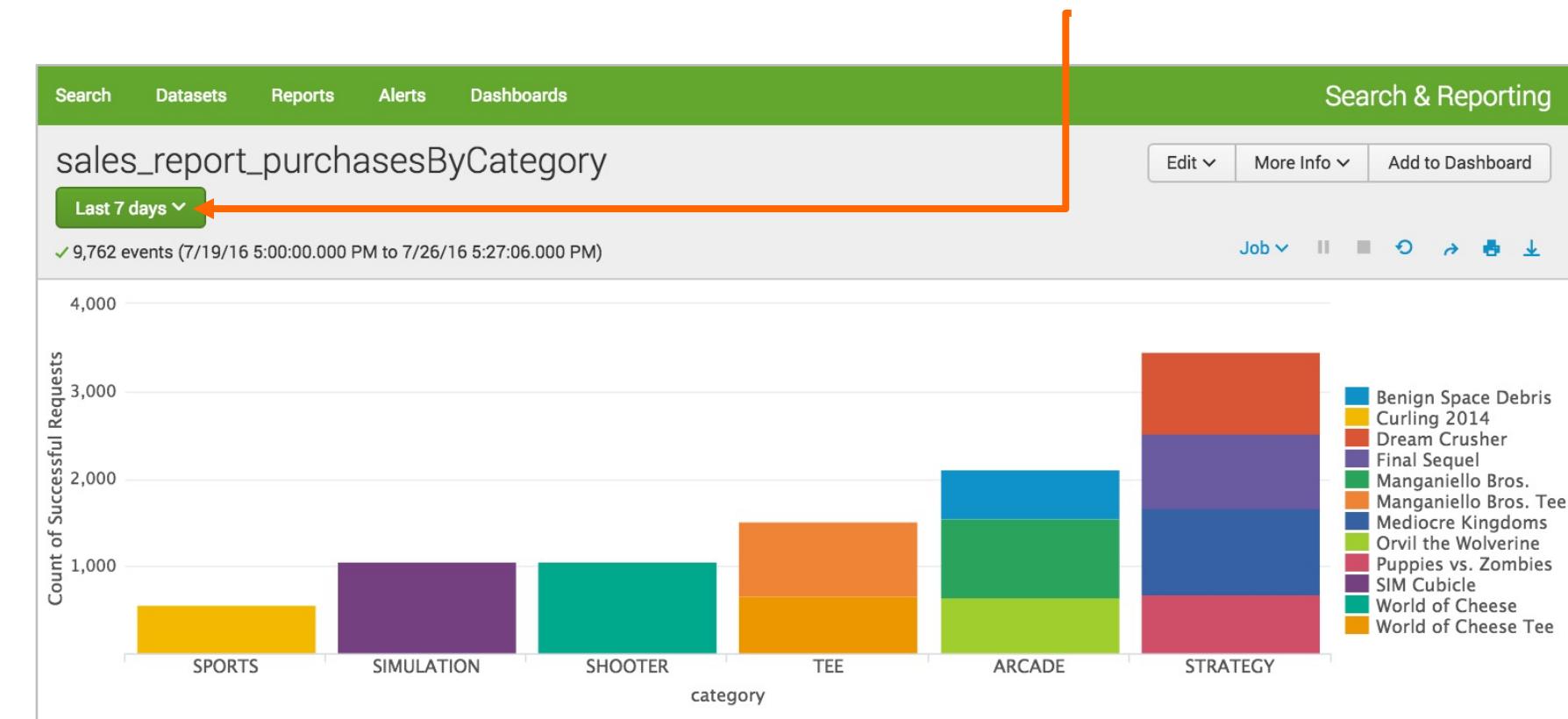
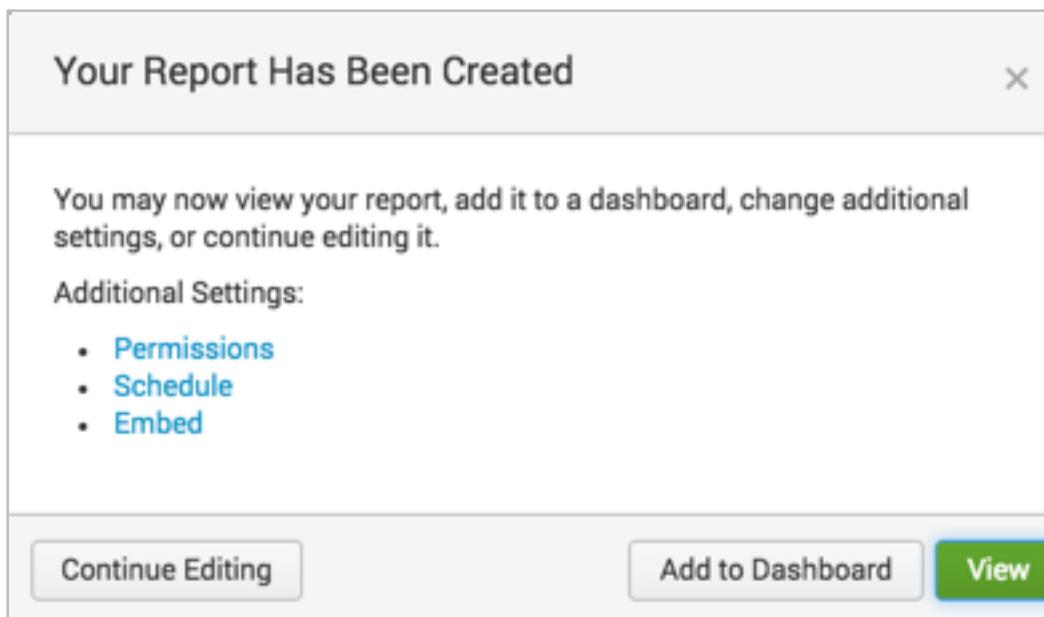
Saving a Pivot

- Pivots can be saved as reports
 - You can choose to include a Time Range Picker in the report to allow people who run it to change the time range (default is Yes)
 - You will learn more about reports later in this course



Saving a Pivot (cont.)

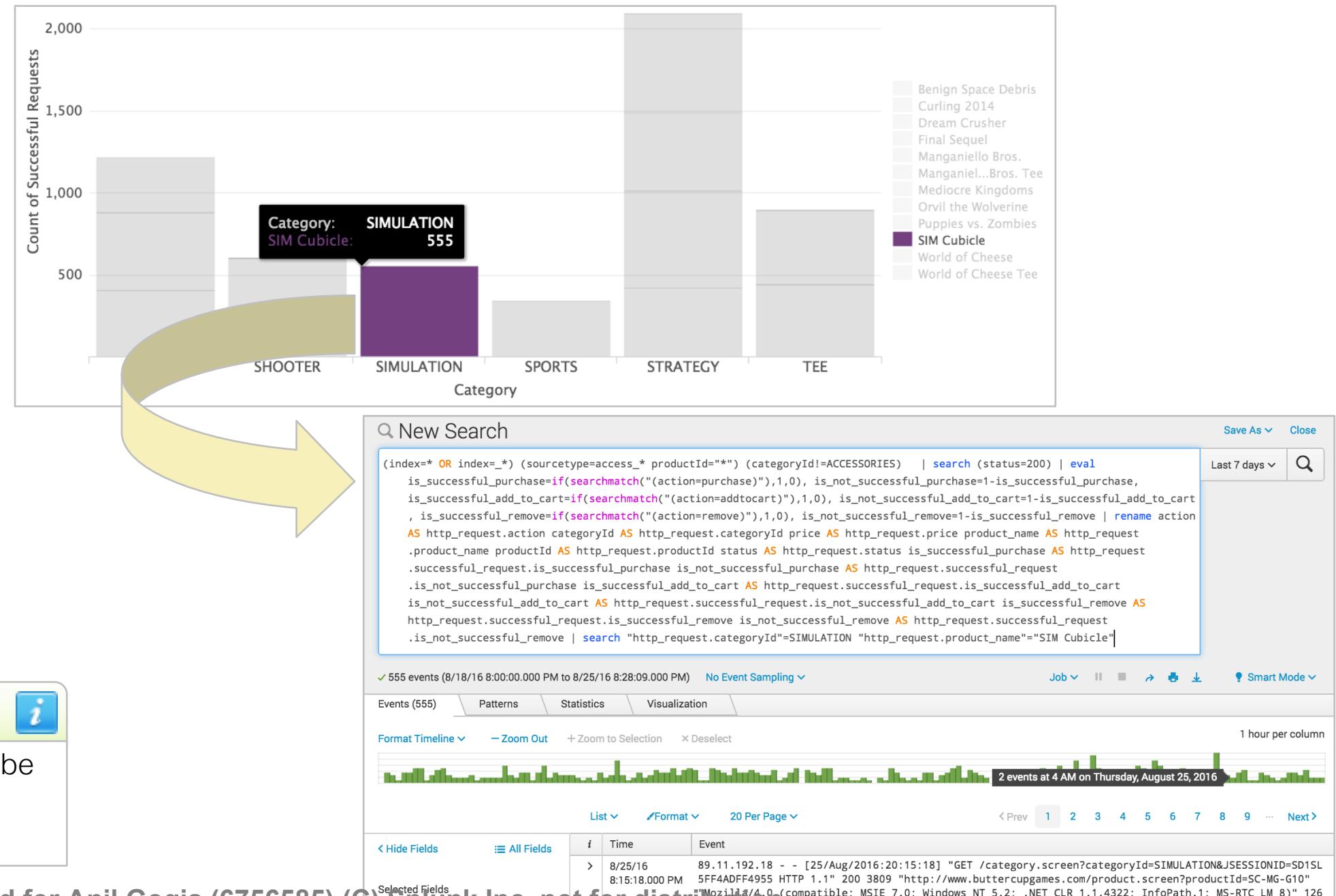
When you click **View**, the report is displayed with a Time Range Picker



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Mouse Actions

- Mouse over an object to reveal its details
- If drilldown is enabled (default), it is possible to click on the object to expose the underlying search



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Instant Pivot Overview

- Instant pivot allows you to utilize the pivot tool without a preexisting data model
 - Instant pivot creates an underlying data model utilizing the search criteria entered during the initial search
- How to create an Instant Pivot
 1. Execute a search (search criteria only, no search commands)
 2. Click the **Statistics** or **Visualization** tab
 3. Click the **Pivot** icon
 4. Select the fields to be included in the data model object
 5. Create the pivot (table or chart)

Open Instant Pivot

The screenshot shows the Splunk interface with the following elements:

- Top Bar:** splunk> App: Search & Re... student16 Messages Settings Activity Help Find
- Header:** Search Datasets Reports Alerts Dashboards Search & Reporting
- Search Bar:** New Search action=purchase Yesterday
- Event Summary:** ✓ 615 events (7/25/16 12:00:00.000 AM to 7/26/16 12:00:00.000 AM) No Event Sampling Job Smart Mode
- Tab Navigation:** Events (615) **(1)** Patterns Statistics Visualization **(2)**
- Visualizations:** Format Timeline Timeline visualization showing event counts over time.
- Selected Fields:** < Hide Fields Selected Fields: action 1, host 3, source 3, sourcetype 1. Interesting Fields: bytes 100+, categoryid 8.
- Pivot Icon:** A green circle with a white icon containing a green arrow pointing up and down, labeled "Pivot".
- Build Instructions:** Build tables and visualizations using multiple fields and metrics without writing searches.
- Modal Dialog: Fields**
 - Which fields would you like to use as a Data Model?
 - All Fields (46) **(3)**
 - Selected Fields (4)
 - Fields with at least 9 % coverage (43)
 -
- Search Commands:** **(4)**
 Use a transforming search and, like timechart or stats, to summarize the data.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Saving a Pivot as a Report

Save As Report

Title: sales_report_purchases

Description: optional

Time Range Picker: Yes

You **2** just save the original search as a data model. This will power the report.

Model Title: purchase data model

Model ID?: purchase_data_model

Note: It is not recommended to manually change the Model ID.

Cancel Save **3**

New Pivot

Save As... Clear Edit Dataset

Report **1**

Dashboard Panel

Filters: Yesterday

Split Columns: host

Split Rows

Column Values: Count of 1469554...

- When saving as a report, the **Model Title** is required
 - This is used to create a data model, which is required by the pivot report
- The **Model ID** is automatically generated based on the **Model Title**

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Add a Pivot to a Dashboard

Similarly, you can save any pivot to a new or existing dashboard

The screenshot illustrates the steps to save a pivot to a dashboard:

- Step 1:** In the top right corner of the pivot interface, a context menu is open with options "Report" and "Dashboard Panel". The "Dashboard Panel" option is highlighted with a red circle labeled "1".
- Step 2:** A modal dialog titled "Save As Dashboard Panel" is displayed. It includes fields for "Dashboard" (set to "New" and "Buttercup Sales Week"), "Panel Title" (optional), "Panel Powered By" (Inline Search), and "Panel Content" (Statistics). A red circle labeled "2" is positioned near the "Panel Powered By" field.
- Step 3:** At the bottom right of the modal, there is a green "Save" button with a red circle labeled "3".

The main area shows a stacked bar chart titled "Successful Requests" with categories ARCADE, SHOOTER, SIMULATION, SPORTS, STRATEGY, and TEE. The Y-axis ranges from 0 to 4,000. The legend lists various product names: Beni..., Curi..., Drean..., Final..., Mang..., Mang..., Medi..., Orvil..., Pupp..., SIM ..., Worl..., Worl... . The chart shows that the STRATEGY category has the highest count of successful requests, followed by ARCADE and TEE.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module 12: Creating and Using Lookups

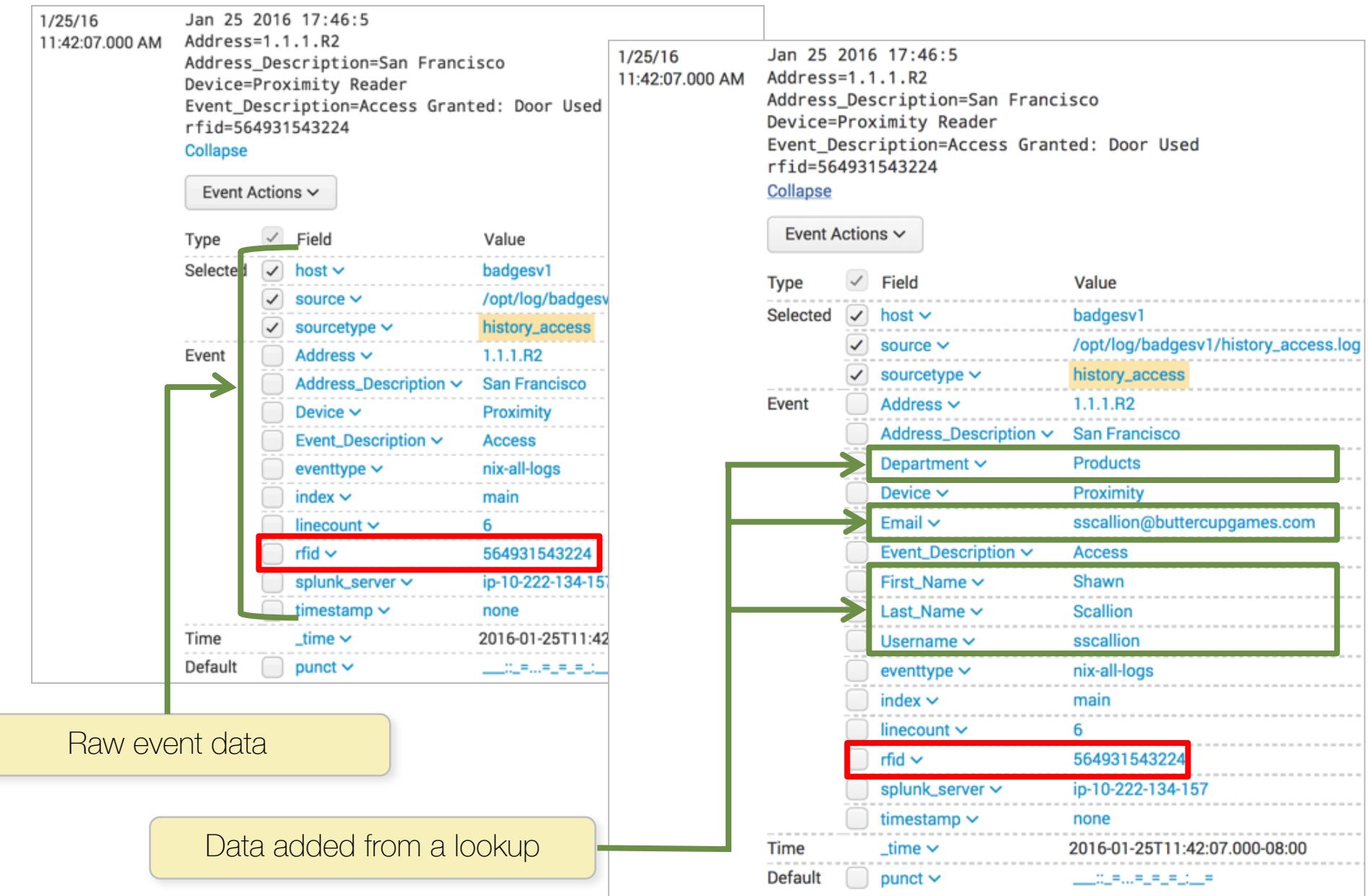
Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module Objectives

- Describe lookups
- Examine a lookup file example
- Create a lookup file and definition
- Configure an automatic lookup
- Use the lookup in searches

Describing Lookups

- There are use cases where static or relatively unchanging data is required for searches, but is not available in the index
- For example, from an RFID in a badge reader event, you can look up employee information



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Describing Lookups (cont.)

- Lookups allow you to add more fields to your events:
 - Provide descriptions for http status codes (“file not found”, “service unavailable”)
 - Define sale prices for products
 - Associate RFIDs with user names, IP addresses, and workstation IDs
- Lookups can be defined in a static.csv file, or it can be the output of a Python script
- After a field lookup is configured, you can use the lookup fields in searches
- The lookup fields also appear in the Fields sidebar
- Lookup field values are case-sensitive by default
 - Admins can change the `case_sensitive_match` option to `false` in transforms.conf

Defining a File-based Lookup

1. Upload the file required for the lookup
2. Define the lookup type
3. Optionally, configure the lookup to run automatically

Lookups

Create and configure lookups.

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

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Lookup File – Example

- This example displays a lookup .csv file used to associate product information with productId
- First row represents field names (header)
productId, product_name, categoryId, price, sale_price, Code
- The productId field exists in the access_combined events
 - This is the **input** field
- All of the fields listed above are available to search after the lookup is defined
 - These are the **output** fields

```
GNU nano 2.3.1          File: products.csv

productId,product_name,categoryId,price,sale_price,Code
DB-SG-G01,Mediocre Kingdoms,STRATEGY,24.99,19.99,A
DC-SG-G02,Dream Crusher,STRATEGY,39.99,24.99,B
FS-SG-G03,Final Sequel,STRATEGY,24.99,16.99,C
WC-SH-G04,World of Cheese,SHOOTER,24.99,19.99,D
WC-SH-T02,World of Cheese Tee,TEE,9.99,6.99,E
PZ-SG-G05,Puppies vs. Zombies,STRATEGY,4.99,1.99,F
CU-PG-G06,Curling 2014,SPORTS,19.99,16.99,G
MB-AG-G07,Manganiello Bros.,ARCADE,39.99,24.99,H
MB-AG-T01,Manganiello Bros. Tee,TEE,9.99,6.99,I
FI-AG-G08,Orvil the Wolverine,ARCADE,39.99,24.99,J
BS-AG-G09,Benign Space Debris,ARCADE,24.99,19.99,K
SC-MG-G10,SIM Cubicle,SIMULATION,19.99,16.99,L
WC-SH-A01,Holy Blade of Gouda,ACCESSORIES,5.99,2.99,M
WC-SH-A02,Fire Resistance Suit of Provolone,ACCESSORIES,3.99,1.99,N
```

Creating a Lookup Table

Settings > Lookups > Lookup table files

1. Click **New**
2. Select a destination app
3. Browse and select the **.csv** file to use for the lookup table
4. Enter a name for the lookup file
5. Save

Add new
Lookups » Lookup table files » Add new

Destination app *
search

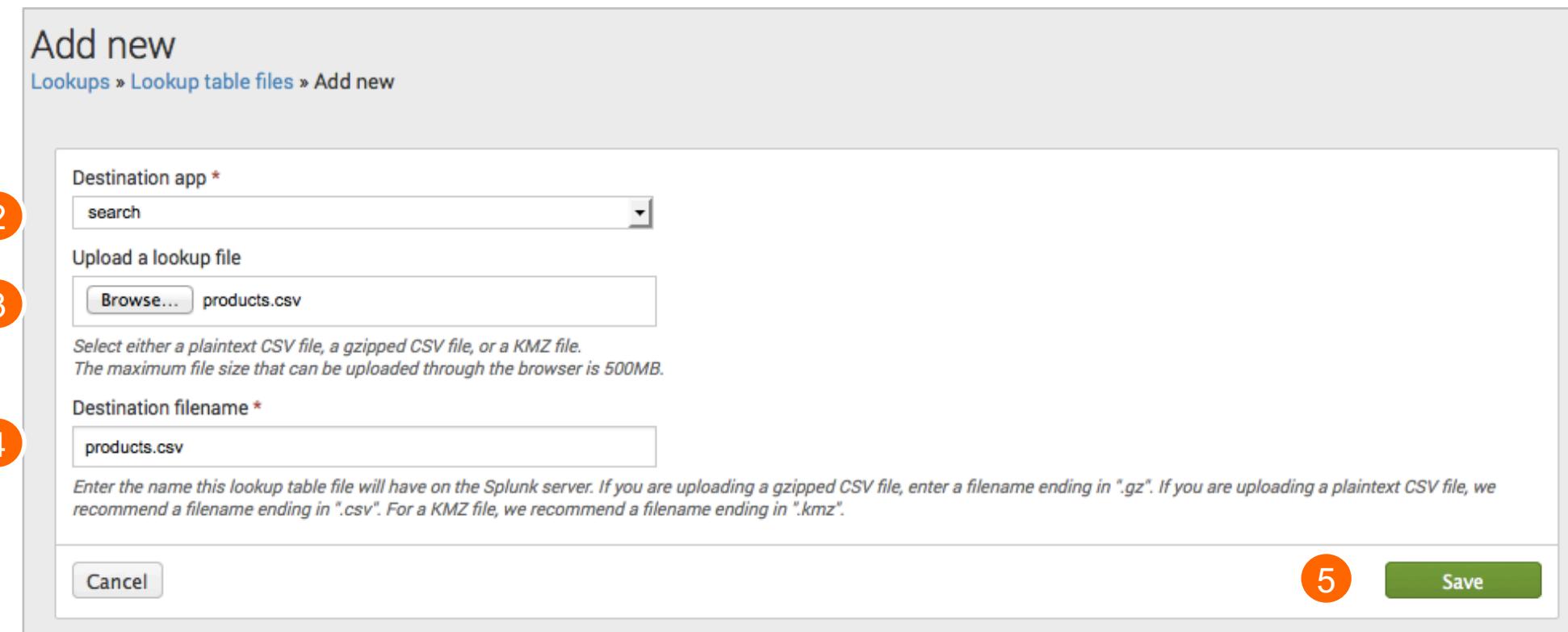
Upload a lookup file
Browse... products.csv

Select either a plaintext CSV file, a gzipped CSV file, or a KMZ file.
The maximum file size that can be uploaded through the browser is 500MB.

Destination filename *
products.csv

Enter the name this lookup table file will have on the Splunk server. If you are uploading a gzipped CSV file, enter a filename ending in ".gz". If you are uploading a plaintext CSV file, we recommend a filename ending in ".csv". For a KMZ file, we recommend a filename ending in ".kmz".

Cancel 5 Save

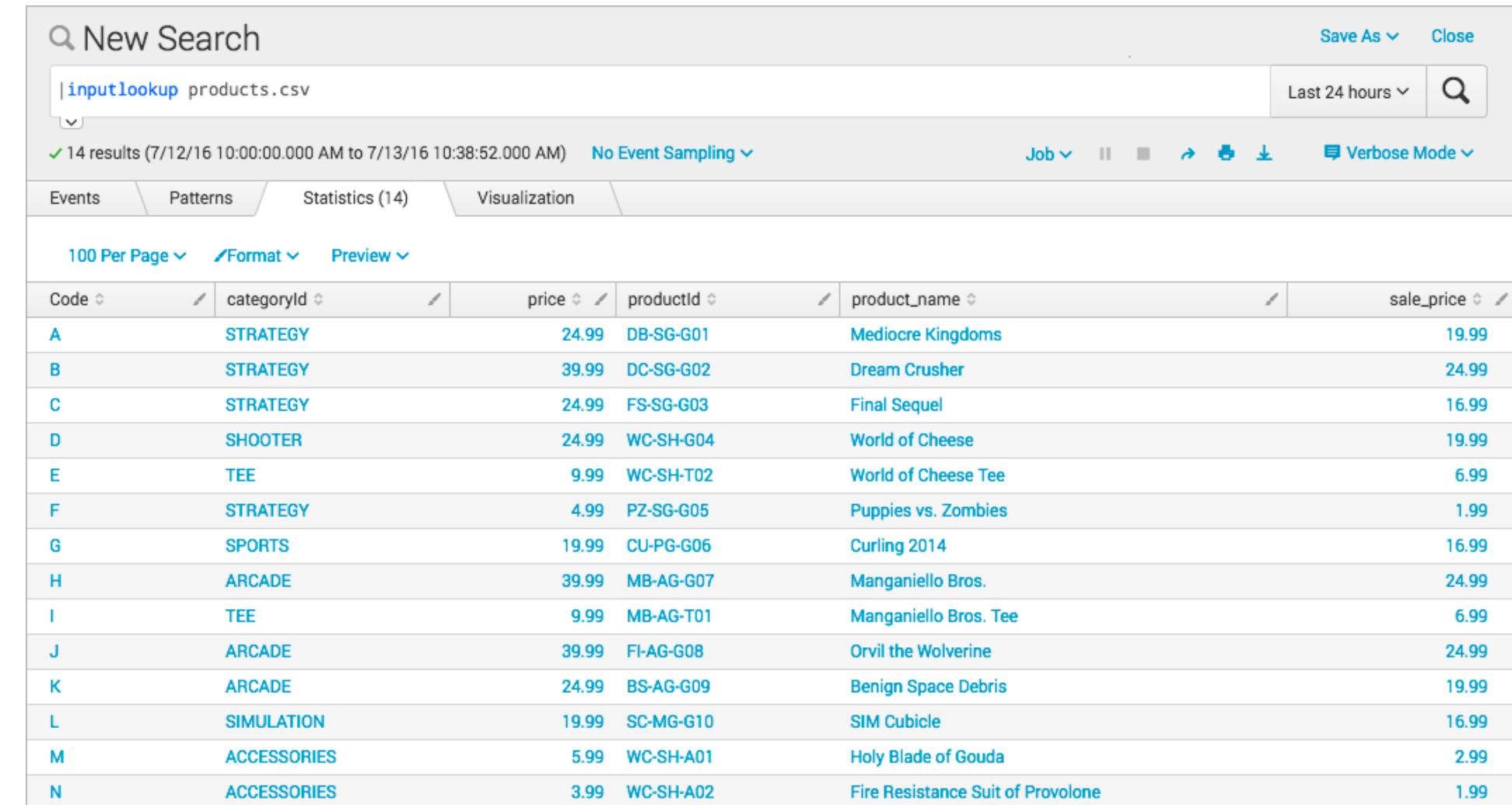


inputlookup Command

- Use the `inputlookup` command to load the results from a specified static lookup
- Useful to:
 - Review the data in the .csv file
 - Validate the lookup

Note 

When using the `inputlookup` command, you can specify the filename ending with .csv or the lookup definition name.



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

- Search Bar:** `|inputlookup products.csv`
- Time Range:** Last 24 hours
- Results:** 14 results (7/12/16 10:00:00.000 AM to 7/13/16 10:38:52.000 AM)
- Event View:** Shows a table with columns: Code, categoryId, price, productId, product_name, and sale_price.
- Data Preview:**

Code	categoryId	price	productId	product_name	sale_price
A	STRATEGY	24.99	DB-SG-G01	Mediocre Kingdoms	19.99
B	STRATEGY	39.99	DC-SG-G02	Dream Crusher	24.99
C	STRATEGY	24.99	FS-SG-G03	Final Sequel	16.99
D	SHOOTER	24.99	WC-SH-G04	World of Cheese	19.99
E	TEE	9.99	WC-SH-T02	World of Cheese Tee	6.99
F	STRATEGY	4.99	PZ-SG-G05	Puppies vs. Zombies	1.99
G	SPORTS	19.99	CU-PG-G06	Curling 2014	16.99
H	ARCADE	39.99	MB-AG-G07	Manganiello Bros.	24.99
I	TEE	9.99	MB-AG-T01	Manganiello Bros. Tee	6.99
J	ARCADE	39.99	FI-AG-G08	Orvil the Wolverine	24.99
K	ARCADE	24.99	BS-AG-G09	Benign Space Debris	19.99
L	SIMULATION	19.99	SC-MG-G10	SIM Cubicle	16.99
M	ACCESSORIES	5.99	WC-SH-A01	Holy Blade of Gouda	2.99
N	ACCESSORIES	3.99	WC-SH-A02	Fire Resistance Suit of Provolone	1.99

Creating a Lookup Definition

Settings > Lookups > Lookup definitions

1. Click **New**
2. Select a destination app
3. Name the lookup definition
4. Select the lookup type, either File-based or External
5. From the drop-down, select a lookup file
6. Save

Add new
Lookups > Lookup definitions > Add new

Destination app
2 search

Name *
3 product_lookup

Type
4 File-based

Lookup file *
5 products.csv
Create and manage lookup table files.

Configure time-based lookup

Advanced options

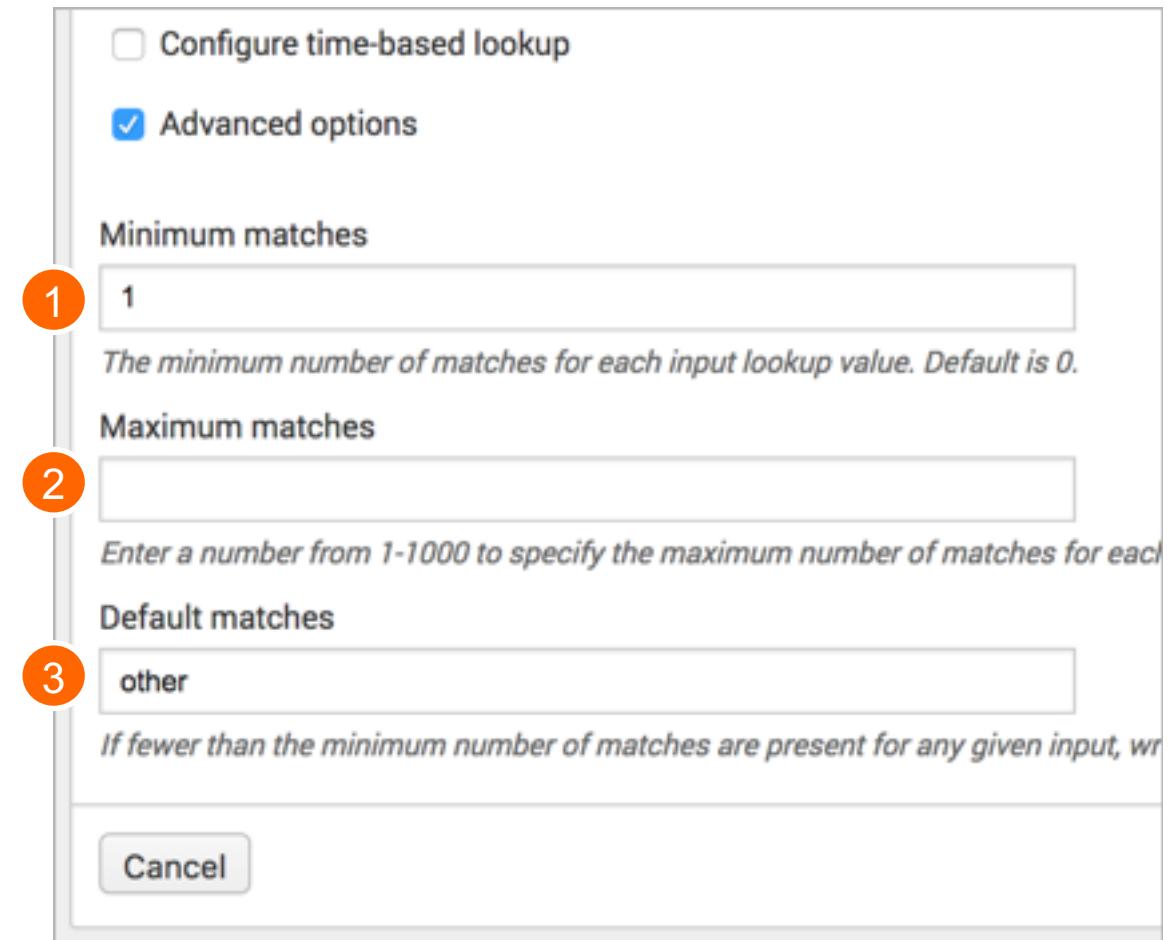
Cancel **Save** 6

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Applying Advanced Options

Under Advanced Options, you can specify:

1. Minimum number of matches for each input lookup value
2. Maximum number of matches for each input lookup value
3. Default value to output, if fewer than the minimum number of matches are present for a given input



lookup Command

- If a lookup is not configured to run automatically, use the `lookup` command in your search to use the lookup fields
- **OUTPUT** - If an **OUTPUT** clause is not specified, all fields in the lookup table that are not the match field are used as output fields
- If **OUTPUT** is specified, the fields overwrite existing fields
- The output lookup fields exist only for the current search
- Use **OUTPUTNEW** when you do not want to overwrite existing fields

[lookup](#) [Help](#) [More »](#)
Explicitly invokes field value lookups.

Examples

There is a lookup table specified in a stanza name 'usertogroup' in transform.conf. This lookup table contains (at least) two fields, 'user' and 'group'. For each event, we look up the value of the field 'local_user' in the table and for any entries that matches, the value of the 'group' field in the lookup table will be written to the field 'user_group' in the event.

... | lookup usertogroup user as local_user OUTPUT group as user_group

Using the lookup Command

New Search

Save As ▾ Close

```
index=web sourcetype=access* action=purchase | lookup product_lookup productID OUTPUT price product_name | stats sum(price) as sales by product_name
```

Last 24 hours ▾

✓ 556 events (10/31/16 9:00:00.000 PM to 11/1/16 9:08:54.000 PM) No Event Sampling ▾ Job ▾

Events (556) Patterns Statistics (14) Visualization

20 Per Page ▾ Format ▾ Preview ▾

Scenario Calculate the sales for each product in the last 24 hours.

product_name	sales
Benign Space Debris	374.85
Curling 2014	599.70
Dream Crusher	799.80
Final Sequel	674.73
Fire Resistance Suit of Provolone	111.72
Holy Blade of Gouda	77.87
Manganiello Bros.	759.81
Manganiello Bros. Tee	209.79
Mediocre Kingdoms	699.72
Orvil the Wolverine	559.86
Puppies vs. Zombies	79.84
SIM Cubicle	359.82
World of Cheese	499.80
World of Cheese Tee	159.84

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Creating an Automatic Lookup

Settings > Lookups > Automatic lookups > New

1. Select the Destination app
2. Enter a Name for the lookup
3. Select the Lookup table definition
4. Select host, source, or sourcetype to apply the lookup and specify the name

Add new

Lookups » Automatic lookups » Add new

Destination app *

1 search

Name *

2 product_auto_lookup

Lookup table *

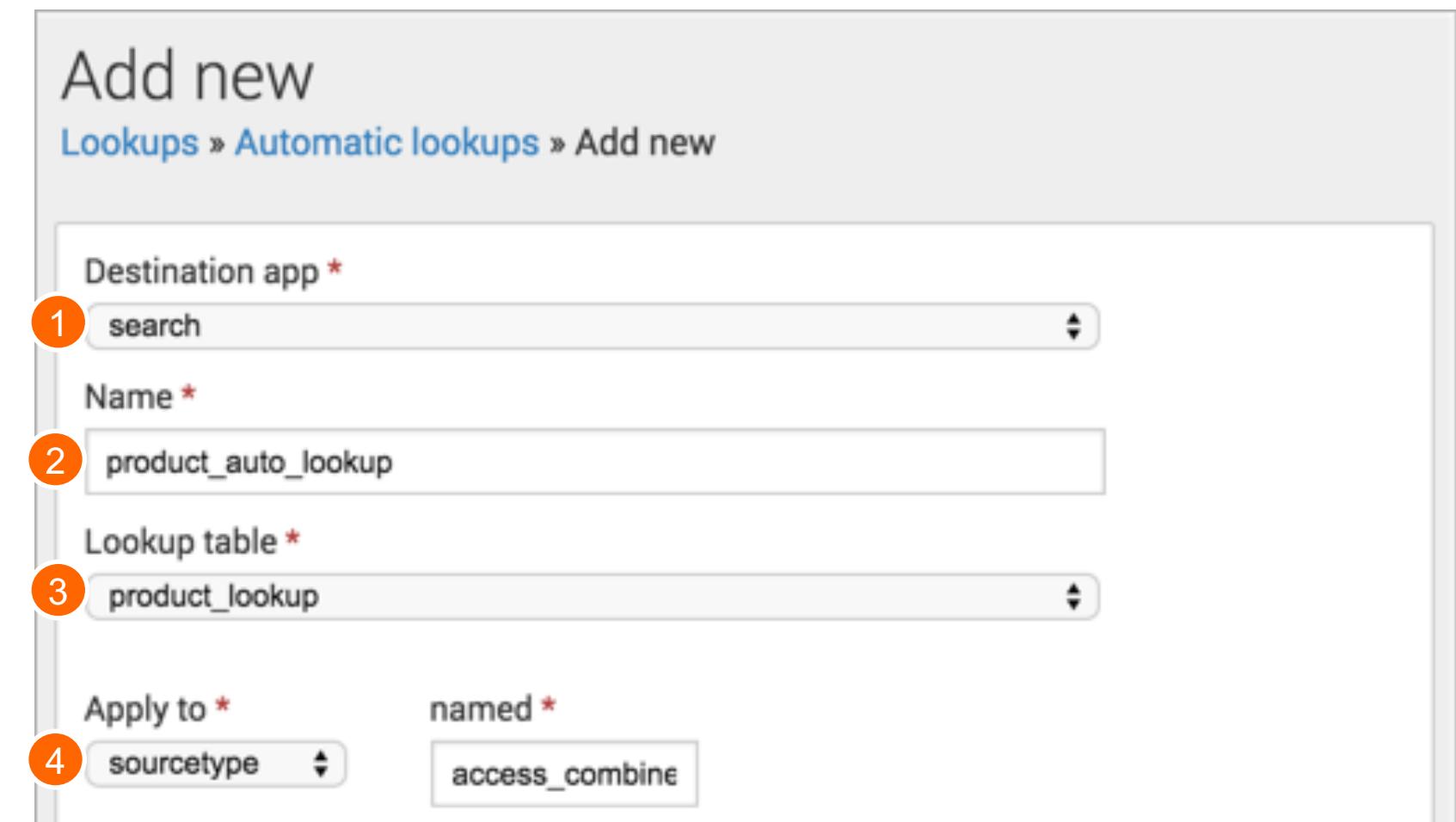
3 product_lookup

Apply to *

4 sourcetype

named *

access_combine



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Creating an Automatic Lookup (cont.)

5. Define the Lookup input fields

- Field(s) that exist in your events that you are relating to the lookup table
 - A. Column name in CSV
 - B. Field name in Splunk, if different from column name

6. Define the Lookup output fields

- Field(s) from your lookup table that are added to the events
 - C. Field name in lookup table
 - D. Name you want displayed in Splunk; otherwise it inherits the column name

7. Save

Lookup input fields

productId A Delete

column name in lookup file

field name in Splunk

Lookup output fields

categoryId C Delete

price D Delete

product_name D Delete

sale_price D Delete

Add another field

Overwrite field values

Cancel Save

Using the Automatic Lookup

To use an automatic lookup, specify the output fields in your search

The screenshot illustrates the use of automatic lookup in Splunk. The search command is:

```
index=web sourcetype=access* action=purchase productId=* | stats sum(price) as sales by productId product_name
```

The output fields specified in the command are highlighted with green boxes: `sum(price)`, `as sales`, `by productId`, and `product_name`. The resulting search results table shows event logs and a summary table.

Event Log Table:

i	Time	Event
>	7/14/16 8:44:40.000 PM	212.235.92.150 - - [14/Jul/2016:20:44:40] "GET /cart.do?action=changequantity&itemId=1&productId=DC-SG-G02&JSESSIONID=SD9SL6FF8ADFF4962 HTTP 1.1" 200 2137 "http://www.buttercupgames.com/oldLink?itemId=EST-21" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5" 557 host = www2 productId = DC-SG-G02 source = /opt/log/www2/access.log sourcetype = access_combined
>	7/14/16 8:44:26.000 PM	212.235.92.150 - - [14/Jul/2016:20:44:26] "POST /oldlink?itemId=EST-17&JSESSIONID=SD9SL6FF8ADFF4962 HTTP 1.1" 200 2983 "http://www.buttercupgames.com/product.screen?productId=PG-G06" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/10.0.1084.52 Safari/536.5" 557 host = www2 productId = PG-G06 source = /opt/log/www2/access.log sourcetype = access_combined

Summary Table:

productId	product_name	sales
BS-AG-G09	Benign Space Debris	499.80
CU-PG-G06	Curling 2014	259.87
DB-SG-G01	Mediocre Kingdoms	824.67
DC-SG-G02	Dream Crusher	799.80
FI-AG-G08	Orvil the Wolverine	519.87

A green bracket on the right side of the summary table indicates that the data was populated via an automatic lookup from the event log table.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Time-based Lookups

- If a field in the lookup table represents a timestamp, you can create a time-based lookup
- In this example, the search retrieved events for February and March and calculated the sales based on the correct unit price for those dates.

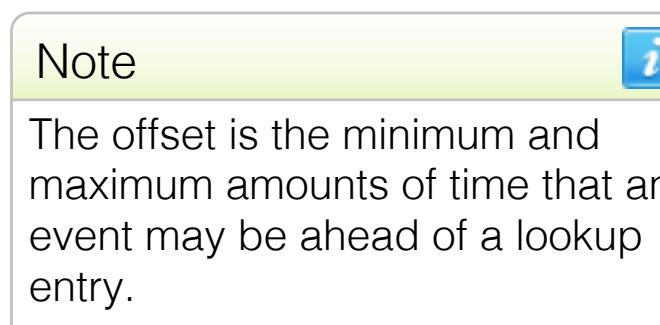
products.csv					
PRODUCTTIME	productId	product_name	categoryId	price	sale_price
1/1/10	DB-SG-G01	Mediocre Kingdoms	STRATEGY	24.99	19.99
1/1/10	DC-SG-G02	Dream Crusher	STRATEGY	39.99	24.99
1/1/10	FS-SG-G03	Final Sequel	STRATEGY	24.99	16.99
1/1/10	WC-SH-G04	World of Cheese	SHOOTER	24.99	19.99
1/1/10	WC-SH-T02	World of Cheese Tee	TEE	9.99	6.99
1/1/10	PZ-SG-G05	Puppies vs. Zombies	STRATEGY	4.99	1.99
1/1/10	CU-PG-G06	Curling 2014	SPORTS	19.99	16.99
1/1/10	MB-AG-G07	Manganiello Bros.	ARCADE	39.99	24.99
1/1/10	MB-AG-T01	Manganiello Bros. Tee	TEE	9.99	6.99
1/1/10	FI-AG-G08	Orvil the Wolverine	ARCADE	39.99	24.99
1/1/10	BS-AG-G09	Benign Space Debris	ARCADE	24.99	19.99
3/1/16	DB-SG-G01	Mediocre Kingdoms	STRATEGY	26.55	21.55
3/1/16	DC-SG-G02	Dream Crusher	STRATEGY	41.55	36.55
3/1/16	FS-SG-G03	Final Sequel	STRATEGY	26.55	21.55
3/1/16	WC-SH-G04	World of Cheese	SHOOTER	26.55	21.55
3/1/16	WC-SH-T02	World of Cheese Tee	TEE	11.55	8.55
3/1/16	PZ-SG-G05	Puppies vs. Zombies	STRATEGY	5.55	2.55
3/1/16	CU-PG-G06	Curling 2014	SPORTS	21.55	18.55
3/1/16	MB-AG-G07	Manganiello Bros.	ARCADE	41.55	26.55
3/1/16	MB-AG-T01	Manganiello Bros. Tee	TEE	11.55	8.55
3/1/16	FI-AG-G08	Orvil the Wolverine	ARCADE	41.55	26.55
3/1/16	BS-AG-G09	Benign Space Debris	ARCADE	26.55	21.55

product_name	Month	price	count	sales	SubTotal Sales
Benign Space Debris	Feb	24.99	402	10,045.98	
Benign Space Debris	Mar	26.55	548	14,549.40	
Benign Space Debris Subtotal					24,595.38
Curling 2014	Feb	19.99	420	8,395.80	
Curling 2014	Mar	21.55	575	12,391.25	
Curling 2014 Subtotal					20,787.05
Dream Crusher	Feb	39.99	691	27,633.09	
Dream Crusher	Mar	41.55	852	35,400.60	
Dream Crusher Subtotal					63,033.69
Final Sequel	Feb	24.99	513	12,819.87	
Final Sequel	Mar	26.55	766	20,337.30	
Final Sequel Subtotal					33,157.17

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Configuring Time-based Lookups

1. Specify the name of the time field in the lookup
2. Enter the strftime format of the time field
3. Define the minimum offset in seconds
 - Default is 0
4. Define the maximum offset in seconds
 - There is no maximum offset by default



Configure time-based lookup

Name of time field *

1 PRODUCTTIME

For time-based lookups, specify the name of the field in the lookup table that represents the timestamp.

Time format

2 %m-%d-%Y

Specify the strftime format of the timestamp field. Default format is UTC time.

Minimum offset

3

The minimum time in seconds that the event time may be ahead of lookup entry time.

Maximum offset

4

The maximum time in seconds that the event time may be ahead of lookup entry time.

Advanced options

Using the Lookup as a Dataset

- A lookup is categorized as a dataset
 - Manage
 - Pivot
 - View the lookup in a search (`inputlookup`)

 Datasets

Use the Datasets listing page to view and manage your existing datasets. Click a dataset name to view its contents. Click Pivot to design a visualization-rich report based on the dataset. Click Explore in Search to extend a dataset in Search and save it as a new report, alert, or dashboard panel.

[Learn more about Datasets.](#)

29 Datasets								
	All	Yours	This App's	Filter by title, description, fields				
i	Title ^	Type	Actions			Owner	App	Sharing
>	geo_attr_countries	lookup definition	Manage	Pivot	Explore in Search	nobody	search	Global
>	geo_attr_countries.csv	lookup table file	Manage	Pivot	Explore in Search	nobody	search	Global
>	geo_attr_us_states	lookup definition	Manage	Pivot	Explore in Search	nobody	search	Global
>	geo_attr_us_states.csv	lookup table file	Manage	Pivot	Explore in Search	nobody	search	Global

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Additional Lookup Options

In addition to creating and using a file-based lookup, you can also:

- Populate a lookup table with search results
 - `-outputlookup` is discussed in more detail in the *Advanced Searching & Reporting* class
- Define a field lookup based on an external command; Python- and binary-based scripts
 - For more information, see the *Knowledge Manager Manual*
docs.splunk.com/Documentation/Splunk/latest/Knowledge/Addfieldsfromexternaldatasources
- Use the Splunk DB Connect app to create lookups with data from external SQL databases

Additional Lookup Options (cont.)

- Use Geospatial lookups to create queries that can be used to generate choropleth map visualizations
<http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Configuregeospatiallookups>
- Populate events with fields from an App Key Value Store (KV Store) collection
 - KV Store lookups can only be invoked through REST endpoints or by using search commands such as lookup, inputlookup, and outputlookup; therefore, cannot be set up as automatic
 - For more information, see the *Knowledge Manager Manual*
<http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/ConfigureKVstorelookups>

Module 13:

Creating Scheduled Reports

and Alerts

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Module Objectives

- Describe scheduled reports and alerts
- Create scheduled reports and alerts
 - Run the underlying search
 - Set the schedule, conditions, and actions
- View fired, scheduled reports and alerts

Using Scheduled Reports

- Scheduled Reports are useful for:
 - Monthly, weekly, daily executive/managerial roll up reports
 - Dashboard performance
 - Automatically sending reports via email

Creating a Scheduled Report

- Create your search
- From the **Save As** menu, select **Report**

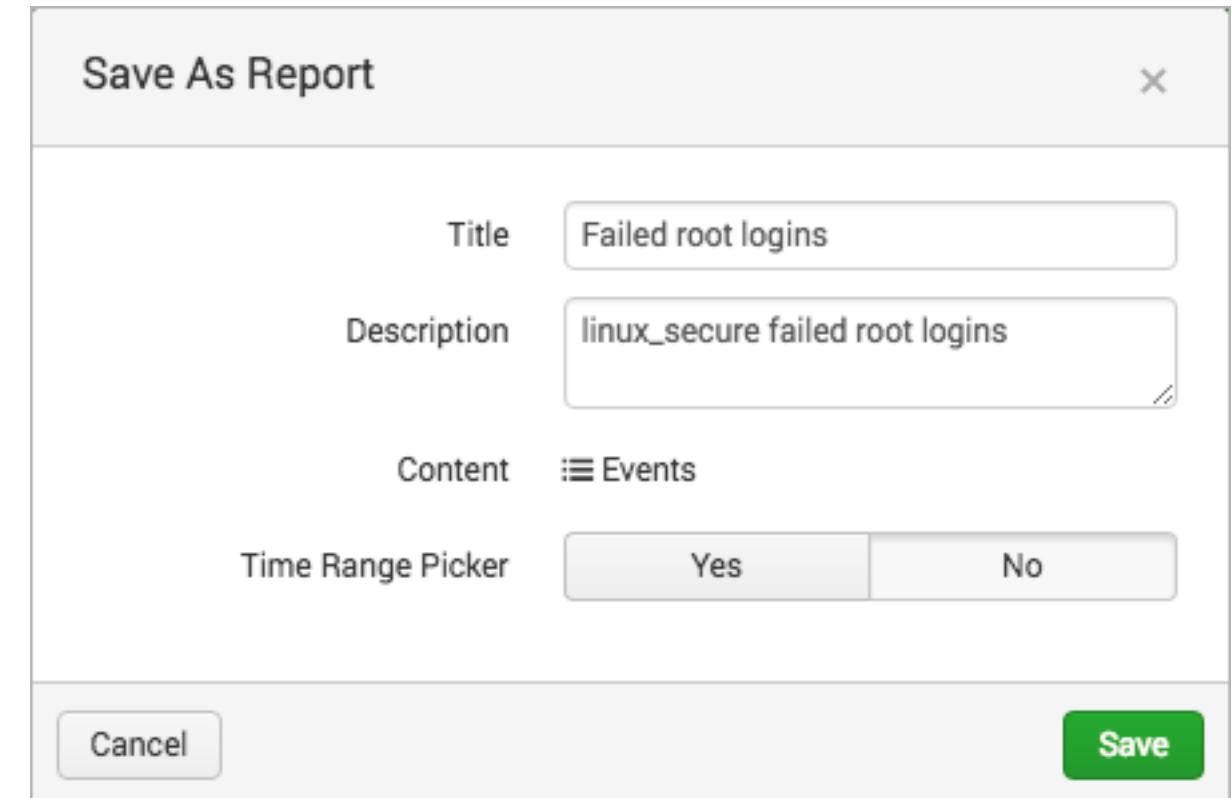
The screenshot shows the Splunk interface with a search bar containing the query "index=web OR index=security fail* root". Below the search bar, a timeline visualization shows green bars representing event intervals. The main area displays a table of event details:

	i	Time	Event
< Hide Fields	All Fields	>	8/18/16 9:45:08 AM Thu Aug 18 2016 16:45:08 www2 sshd[4167]: Failed password for root from 91.214.92.22 port 4499 ssh2 eventtype = errOr error eventtype = failed_login eventtype = failed_privileged_logins eventtype = sshd_authentication authentication remote eventtype = nix-all-logs eventtype = nix_errors error host = www2 port = 4499 source = /opt/log/www2/secure.log sourcetype = linux_secure tag = authentication tag = error tag = privileged tag = remote
Selected Fields	a eventtype 6 a host 4 # port 100+ a source 4 a sourcetype 1 a tag 4	>	8/18/16 9:42:43 AM Thu Aug 18 2016 16:42:43 www1 sshd[3438]: Failed password for root from 91.208.184.24 port 2820 ssh2 eventtype = errOr error eventtype = failed_login eventtype = failed_privileged_logins eventtype = sshd_authentication authentication remote eventtype = nix-all-logs eventtype = nix_errors error host = www1 port = 2820 source = /opt/log/www1/secure.log sourcetype = linux_secure tag = authentication tag = error tag = privileged tag = remote
Interesting Fields	a action 1		

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Creating a Scheduled Report (cont.)

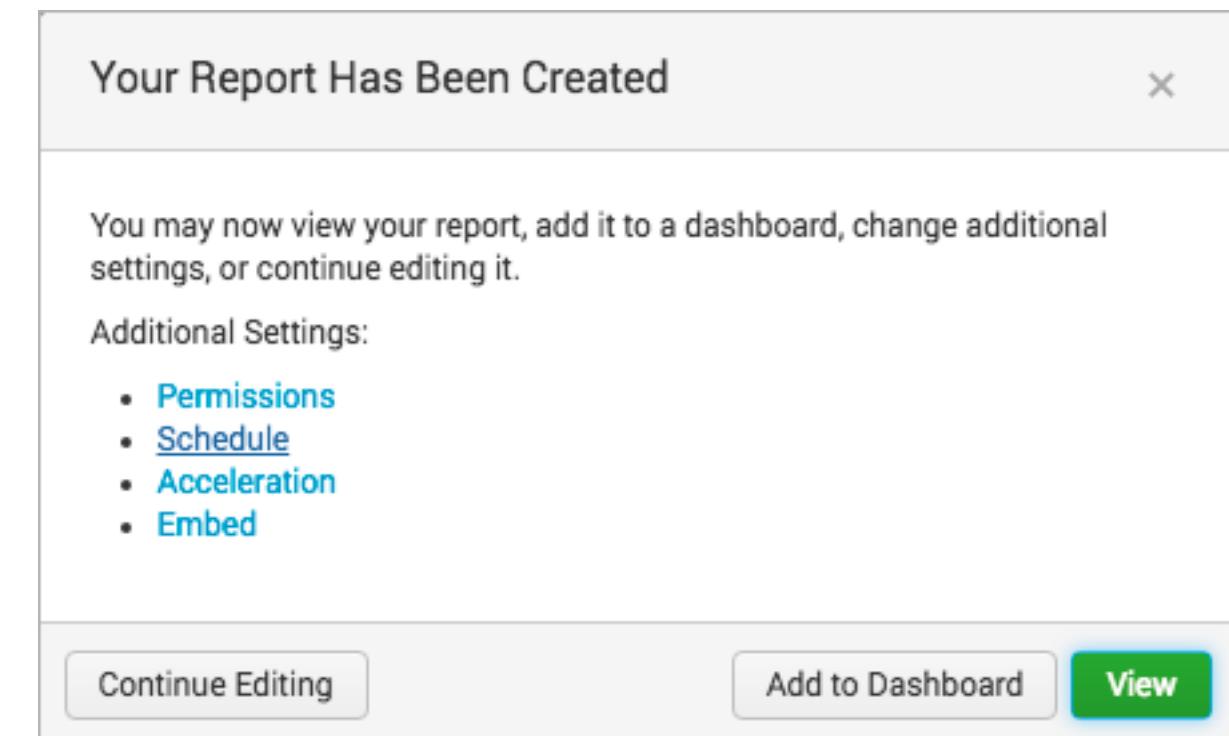
- **Title** – enter a title for your report
- **Description** – provide a description
- **Time Range Picker** – you can add a time range picker to the report
- Click **Save**



Note i
When you schedule a report, the Time Range Picker will not be available.

Creating a Scheduled Report (cont.)

After the report is created, click **Schedule**



Creating a Scheduled Report – Define Schedule

- **Schedule Report** – select this checkbox
- **Schedule** – select the frequency to run the report
 - Run every hour
 - Run every day
 - Run every week
 - Run every month
 - Run on Cron Schedule

Edit Schedule

Report Failed root logins

Schedule Report Learn More ↗

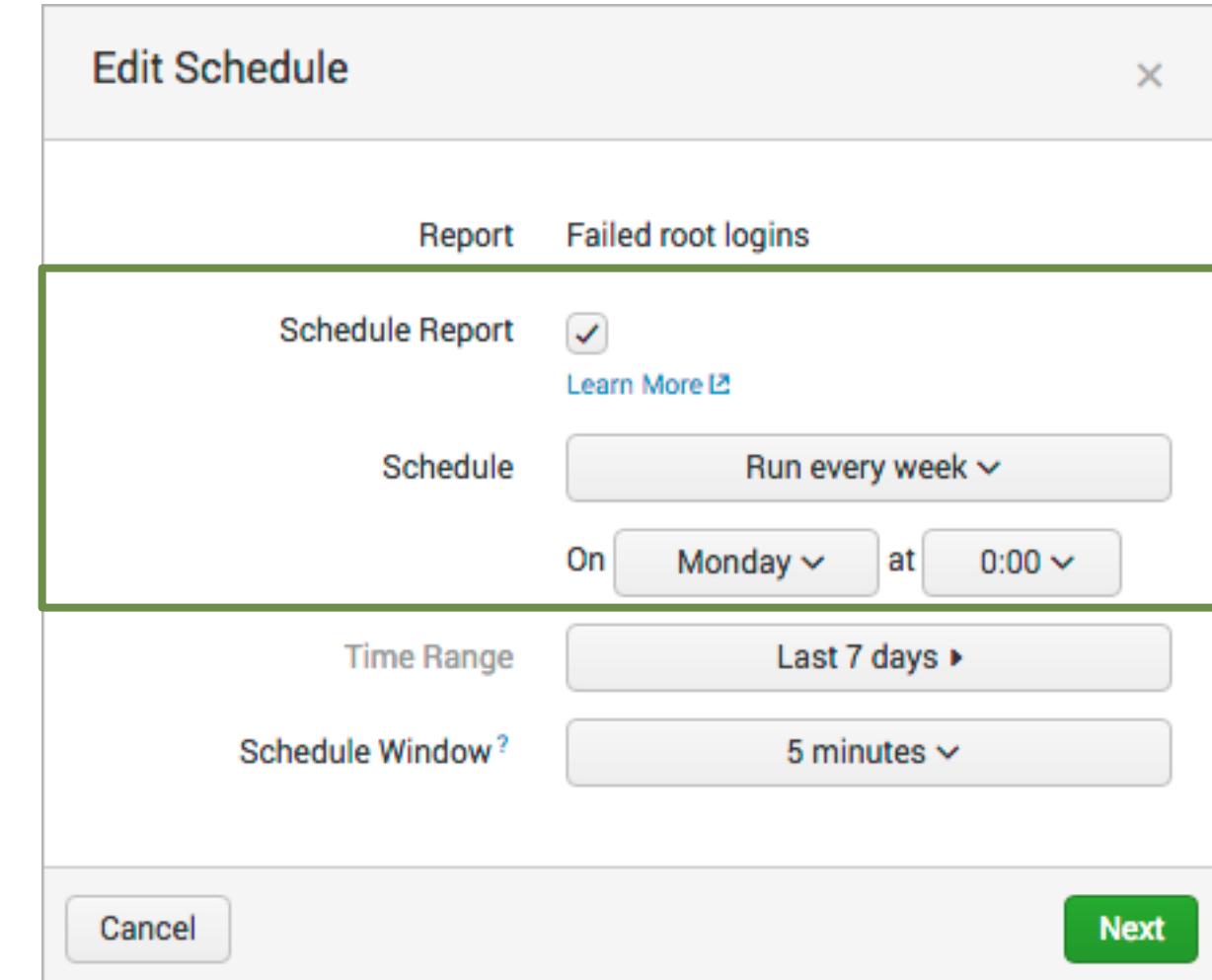
Schedule Run every week

On Monday at 0:00

Time Range Last 7 days

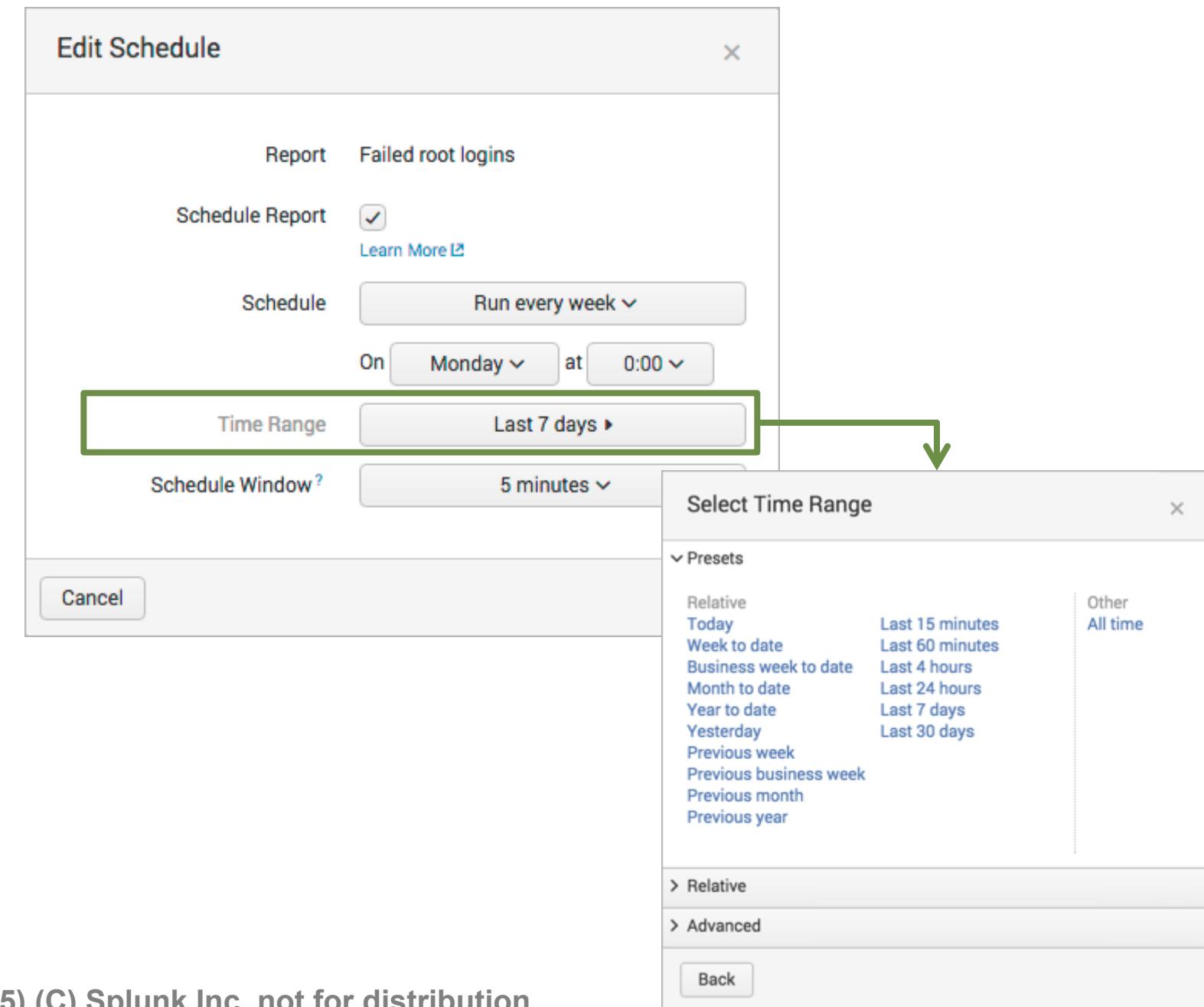
Schedule Window? 5 minutes

Cancel Next



Creating a Scheduled Report – Select Time Range

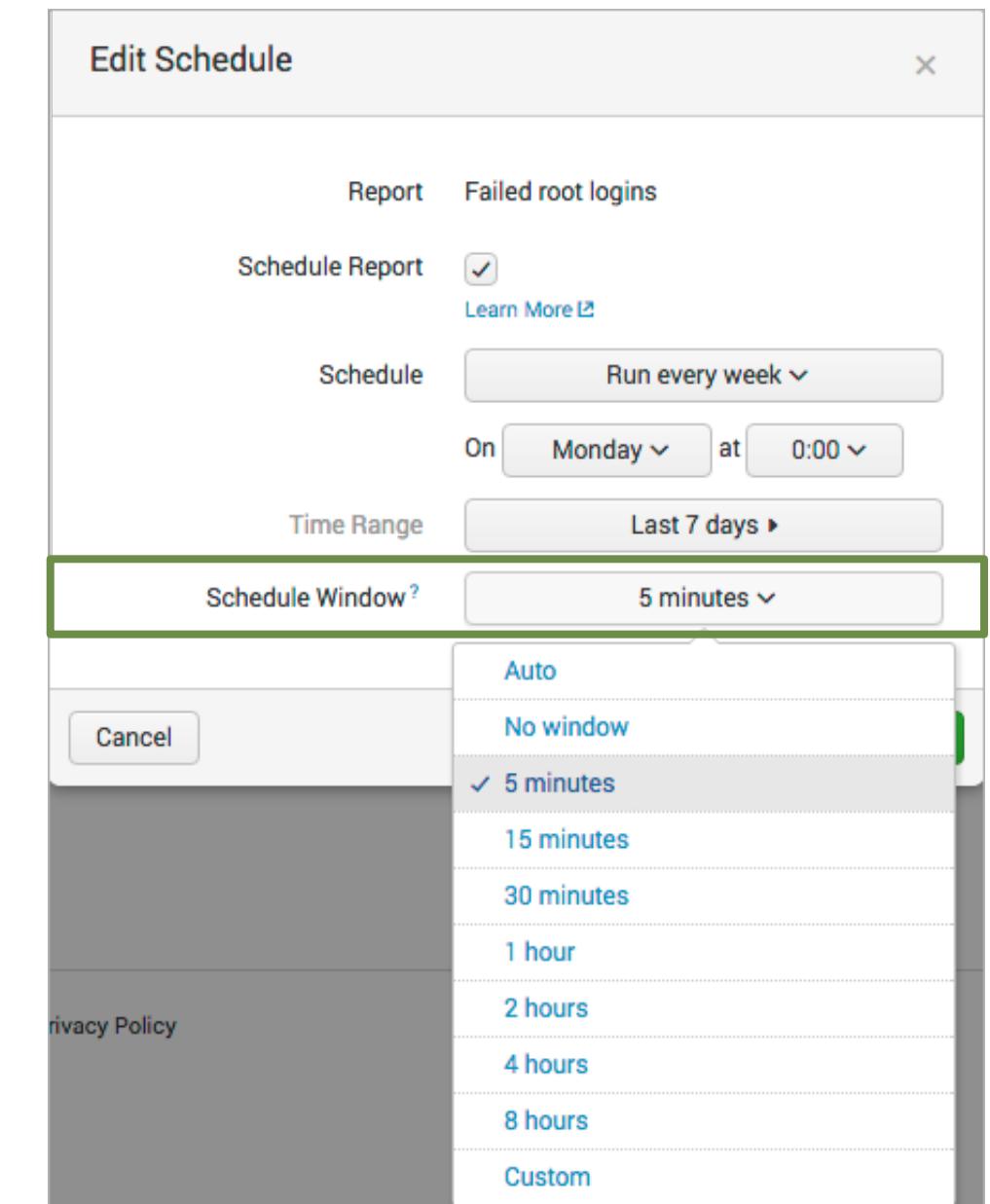
- **Time Range** – By default, the search time range is used
 - Click the time range button to change the time range
 - You can select a time range from Presets, Relative, or Advanced
 - Typically, the time range is relative to the Schedule



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Creating a Scheduled Report – Schedule Window

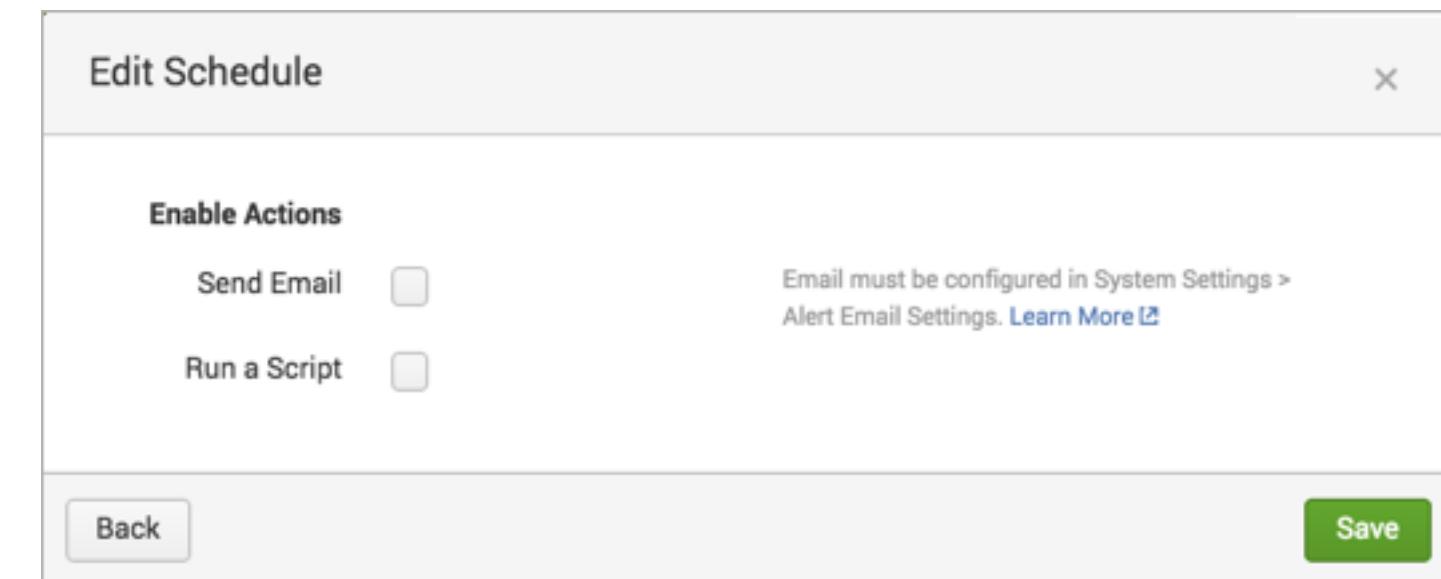
- **Schedule Window** – This setting determines a time frame to run the report
 - If there are other reports scheduled to run at the same time, you can provide a window in which to run the report
 - This setting provides efficiency when scheduling several reports to run
- After you configure the schedule report, click **Next**



Creating a Scheduled Report – Enable Actions

- **Enable Actions**

- **Send Email:** When a report runs, an email is sent to the specified recipient(s)
- **Run a script:** A script is launched when a report runs



Creating a Scheduled Report – Send Email

1. Enter addresses in the **To** field, separated by a comma
2. Set the priority
3. Edit or keep the default subject
 - The \$name\$ variable includes the name of the report
 - In addition to a message, you can include other options like an inline table of the results, etc.
4. Define the email text type
5. After you have configured the actions, click **Save**

Edit Schedule

Enable Actions

Send Email

To Email must be configured in System Settings > Alert Email Settings. [Learn More](#)

Email Priority

Subject The email subject, recipients and message can include tokens that insert text based on the results of the search. [Learn More](#)

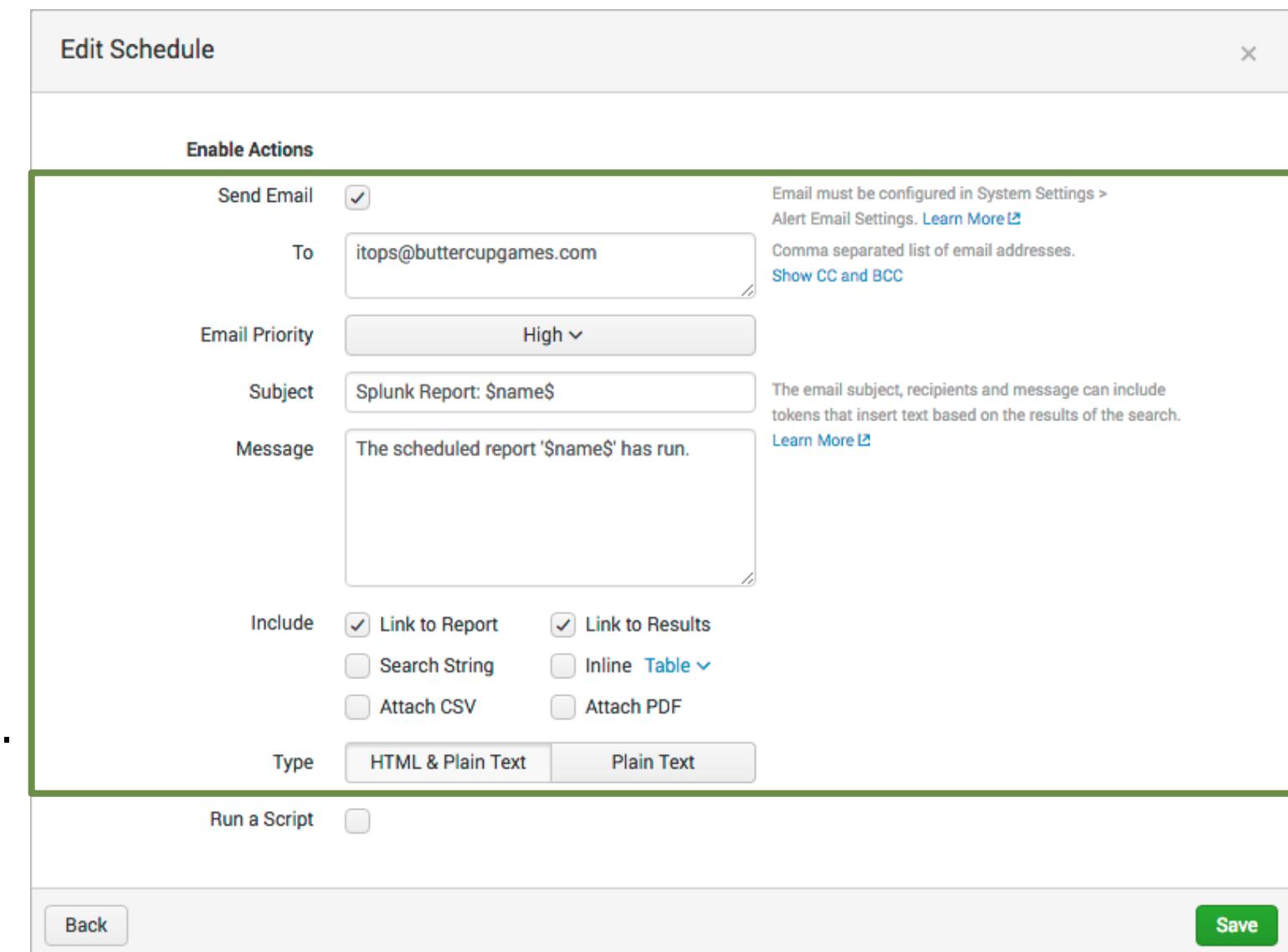
Message

Include Link to Report Link to Results
 Search String Inline Table
 Attach CSV Attach PDF

Type HTML & Plain Text Plain Text

Run a Script

[Back](#) [Save](#)

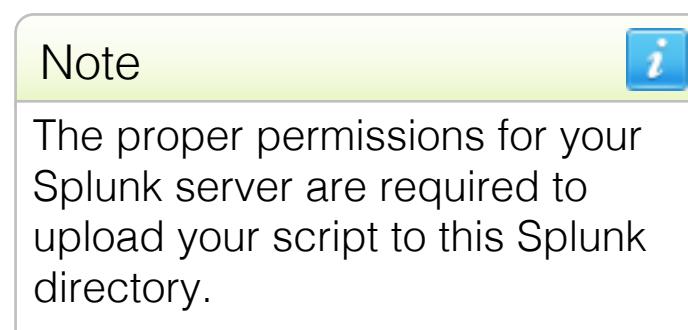


Creating a Scheduled Report – Run a Script

1. Enter the file name of the script

- The script must reside in the
`$SPLUNK_HOME/bin/scripts`
directory

2. Click **Save**



Edit Schedule

Enable Actions

Send Email

To: itops@buttercupgames.com

Email Priority: High

Subject: Splunk Report: \$name\$

Message: The scheduled report '\$name\$' has run.

Include

Link to Report Link to Results

Search String Inline Table

Attach CSV Attach PDF

Type: HTML & Plain Text Plain Text

Run a Script

Run a Script

Filename: loginerrorscript.sh

Located in \$SPLUNK_HOME/bin/scripts or \$SPLUNK_HOME/etc/search/bin/scripts

Save

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Managing Reports – Edit Permissions

Display For determines who sees the scheduled report

The image shows two screenshots of the Splunk interface. On the left, the 'Reports' page displays three reports: 'Failed logins', 'Failed root logins', and 'Weekly T-shirt Sales'. The 'Failed root logins' report is selected. A context menu is open over this report, with 'Edit Permissions' highlighted and surrounded by a green box. A large green arrow points from this menu item to the 'Edit Permissions' dialog on the right. The 'Edit Permissions' dialog shows the report details: 'Report' is 'Failed root logins', 'Owner' is 'cfarrell', and 'App' is 'search'. The 'Display For' section is selected and shows options: 'Owner' (selected), 'App', and 'All apps'. Below this, the 'Run As' section shows 'Owner' with a link to 'Learn More'. The 'Read' and 'Write' checkboxes for 'Everyone', 'power', 'student', and 'user' are all unchecked. At the bottom are 'Cancel' and 'Save' buttons.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Managing Reports – Edit Permissions (cont.)

- **Run As** – determines which user profile is used at run time
 - Owner – all data accessible by the owner appears in the report
 - User – only data allowed to be accessed by the user role appears

The screenshot shows the Splunk Reports interface. At the top, it says "Reports" and provides instructions: "Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data." Below this, there's a table with three reports: "Failed logins", "Failed root logins", and "Weekly T-shirt Sales". For each report, columns show "Actions", "Owner", "App", "Sharing", and "Embedding". A dropdown menu is open over the "Edit Description" link for the "Weekly T-shirt Sales" report. The menu items are: "Edit Permissions" (highlighted with a green box and a mouse cursor), "Edit Schedule", "Edit Acceleration", "Clone", "Embed", and "Delete". A large green arrow points from this menu to the "Edit Permissions" section of the "Edit Permissions" dialog box on the right.

The screenshot shows the "Edit Permissions" dialog box for the "Failed root logins" report. It has tabs for "Report" (selected) and "Failed root logins", "Owner" (cfarrell), "App" (search), and "Display For" (Owner, App selected). The "Run As" section is highlighted with a green box. It shows "Owner" selected under "Run As". The "Learn More" link is visible. The main table lists users and their permissions: "Everyone" (Read checked, Write checked), "power" (Read checked, Write checked), "student" (Read checked, Write checked), and "user" (Read checked, Write checked). At the bottom are "Cancel" and "Save" buttons.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Managing Reports – Embed

- To access the report results from a webpage, click **Edit > Embed**
 - Before a report can be embedded, it must be scheduled

The screenshot illustrates the steps to enable report embedding:

- In the "Reports" dashboard, a context menu is open for the "Failed logins" report. The "Embed" option is highlighted with a green box and an arrow.
- A modal dialog titled "Enable Report Embedding" appears, asking if the user is sure they want to enable embedding. It contains the message: "Are you sure you want to enable embedding for this report? An embedded report can be viewed by anyone with access to the web page(s) in which it is inserted." There are "Cancel" and "Enable Embedding" buttons.
- If "Enable Embedding" is clicked, the "Embed" panel on the right is displayed. It contains a warning: "Embedded Report will not have data until the scheduled search runs." Below is a code block for an iframe:

```
<iframe height="636" width="480" frameborder="0" src="http://54.184.179.177/en-US/embed?s=%2FservicesNS%2Fcfarrell%2Fsearch%2Fsaved%2Fsearches%2FFailed%2520root%2520logins&oid=ysj0DUnWD_ynve3LI9ICrl%5EowLIA%5ERHU4z3xrNeQE74cqmn3ofHb0Y5izPEtrZBDt%5EMGpq6KXrEZQu%5EqK2BHx5qsKWJeEsp"/>
```

Below the code is a link to "Disable embedding" and a "Done" button.

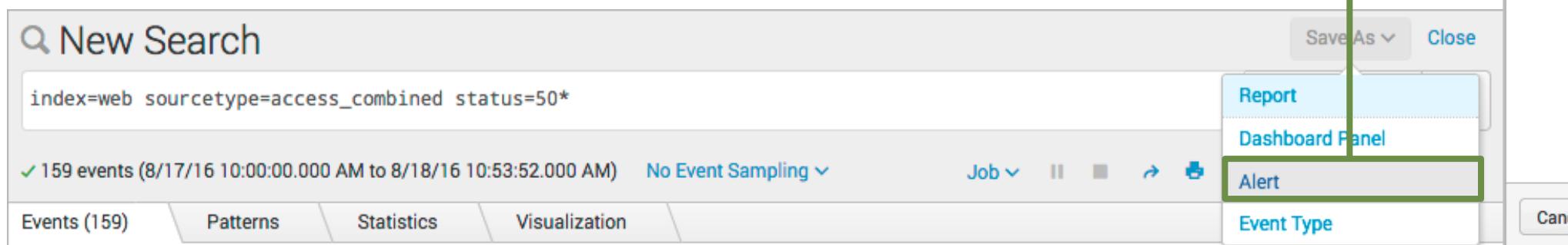
Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Alerting Overview

- Splunk alerts are based on searches that can run either:
 - On a regular **scheduled interval**
 - In **real-time**
- Alerts are triggered when the results of the search meet a specific condition that you define
- Based on your needs, alerts can:
 - List in triggered alerts
 - Send emails
 - Trigger scripts
 - Use a webhook
 - Run a custom alert

Creating an Alert

- Run a search
 - In this example, you're searching for server errors: any http request status that begins with 50 over the last 5 minutes
- Select **Save As > Alert**
- Give the alert a Title and Description



The screenshot shows the 'Save As Alert' dialog box. The 'Settings' section is highlighted with a green border. It contains the following fields:

- Title: Web server errors
- Description: Alerts when http status 50* events are returned
- Permissions: Private (selected)
- Alert type: Scheduled (selected)
- Trigger Conditions: Trigger alert when: Per-Result
- Throttle?:
- Trigger Actions: + Add Actions

A green arrow points from the 'Alert' option in the search interface's context menu to the 'Alert' button in this dialog box.

Setting Alert Permissions

- Set the alert permissions
 - **Private** – only you can access, edit, and view triggered alerts
 - **Shared in app**
 - ▶ All users of the app can view triggered alerts
 - ▶ By default, everyone has read access and power has write access to the alert

Save As Alert X

Settings	
Title	Web server errors
Description	Alerts when http status 50* events are returned
Permissions Shared in App Private	
Alert type Scheduled Real-time	
Trigger Conditions	
Trigger alert when	Per-Result ▼
Throttle ? □	
Trigger Actions	
+ Add Actions ▼	
Cancel	Save

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Choosing Real Time or Scheduled Alert Type

Choose an **Alert type** to determine how Splunk searches for events that may match your alert

- **Scheduled** alerts
 - Search runs at a defined interval
 - Evaluates trigger condition when the search completes
- **Real-time** alerts
 - Search runs constantly in the background
 - Evaluates trigger conditions within a window of time based on the conditions you define

Save As Alert

Settings

Title: Web server errors

Description: Alerts when http status 50* events are returned

Permissions: Private Shared in App

Alert type Scheduled Real-time

Trigger Conditions

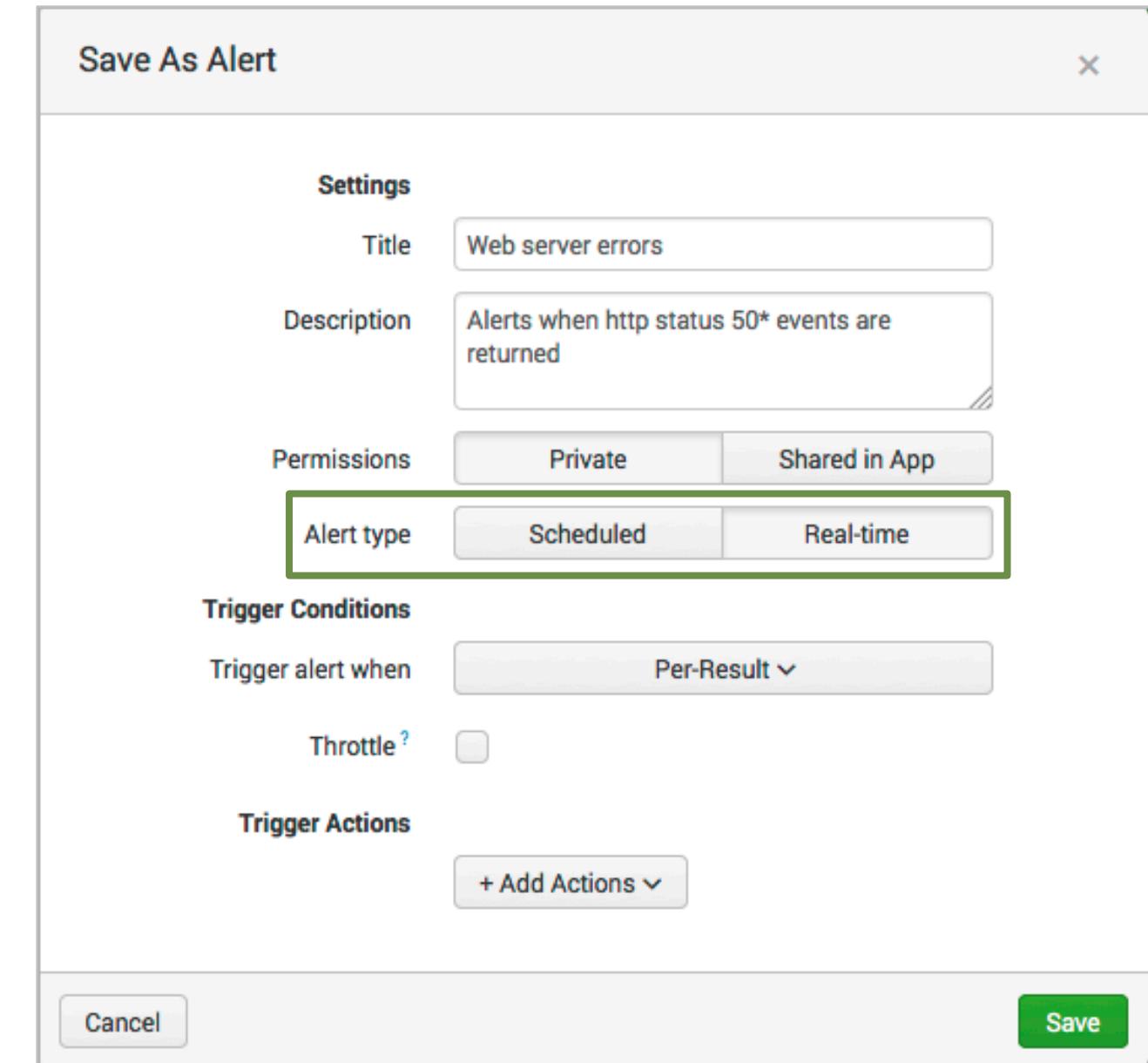
Trigger alert when: Per-Result

Throttle?

Trigger Actions

+ Add Actions

Cancel Save



Setting the Alert Type – Scheduled

- From the frequency menu, choose to run the search every hour, day, week, month, or on a cron schedule
 - For the scheduled interval options, select the time the search will run
 - For cron schedule, define the cron expression

Save As Alert

Settings

Title: Web server errors

Description: Alerts when http status 50* events are returned

Permissions: Private Shared in App

Alert type: **Scheduled** Real-time

Earliest: Run on Cron Schedule

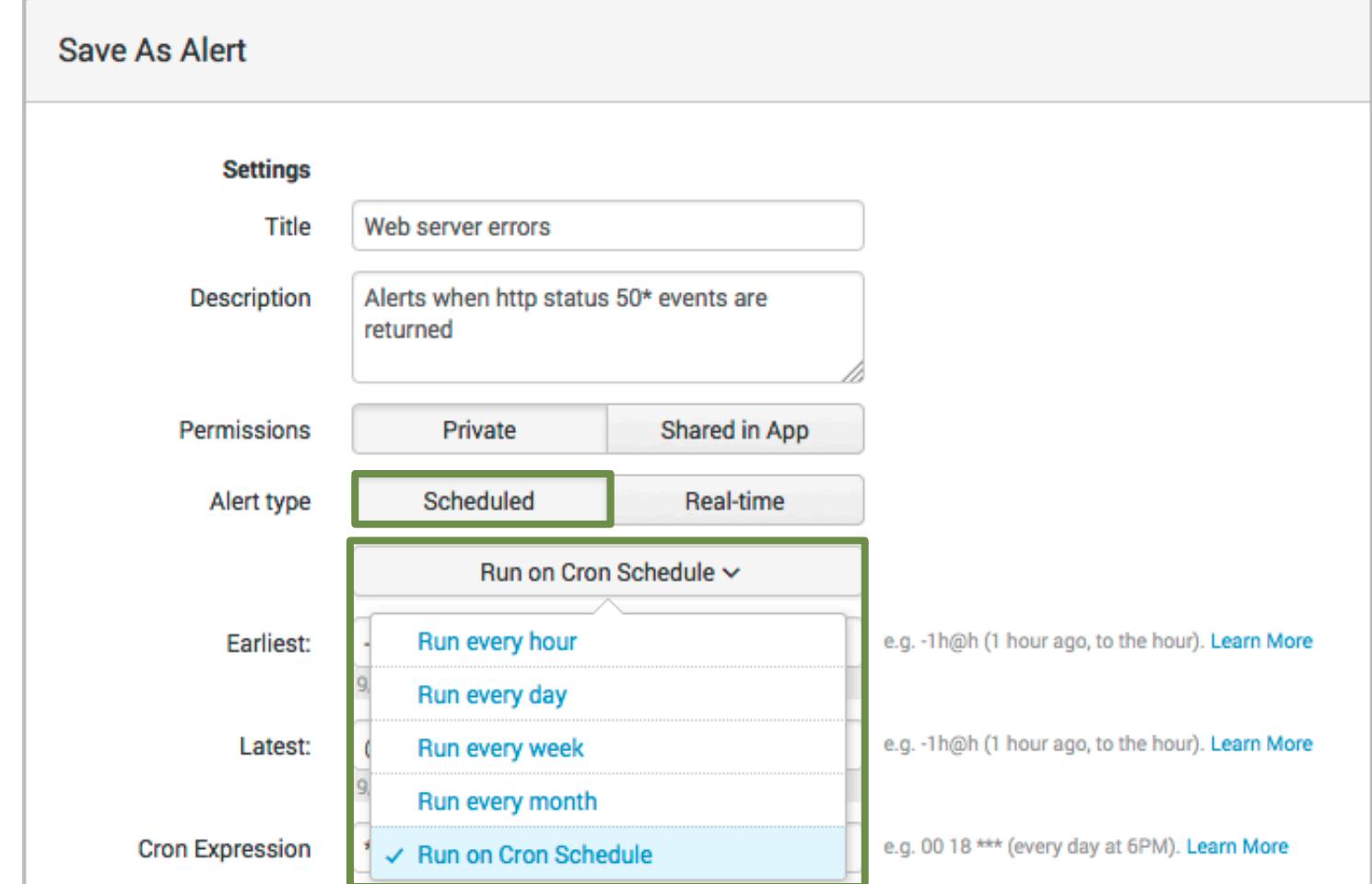
Latest: Run on Cron Schedule

Cron Expression: **Run on Cron Schedule**

e.g. -1h@h (1 hour ago, to the hour). [Learn More](#)

e.g. -1h@h (1 hour ago, to the hour). [Learn More](#)

e.g. 00 18 *** (every day at 6PM). [Learn More](#)



Setting Trigger Conditions – Scheduled

- For the cron schedule, enter the **earliest** and **latest** values to define the time range of the results
- Set trigger conditions for scheduled alerts (same steps outlined for real-time alerts)
 - The alert examines the complete results set after the search is run

Save As Alert

Settings

Title: Web server errors

Description: Alerts when http status 50* events are returned

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run on Cron Schedule

Earliest: -5m@m
9/30/15 11:05:00.000 PM

Latest: @m
9/30/15 11:10:00.000 PM

Cron Expression: */5 * * * *
e.g. 00 18 *** (every hour)

Trigger Conditions

Trigger alert when: Number of Results

is greater than: 2

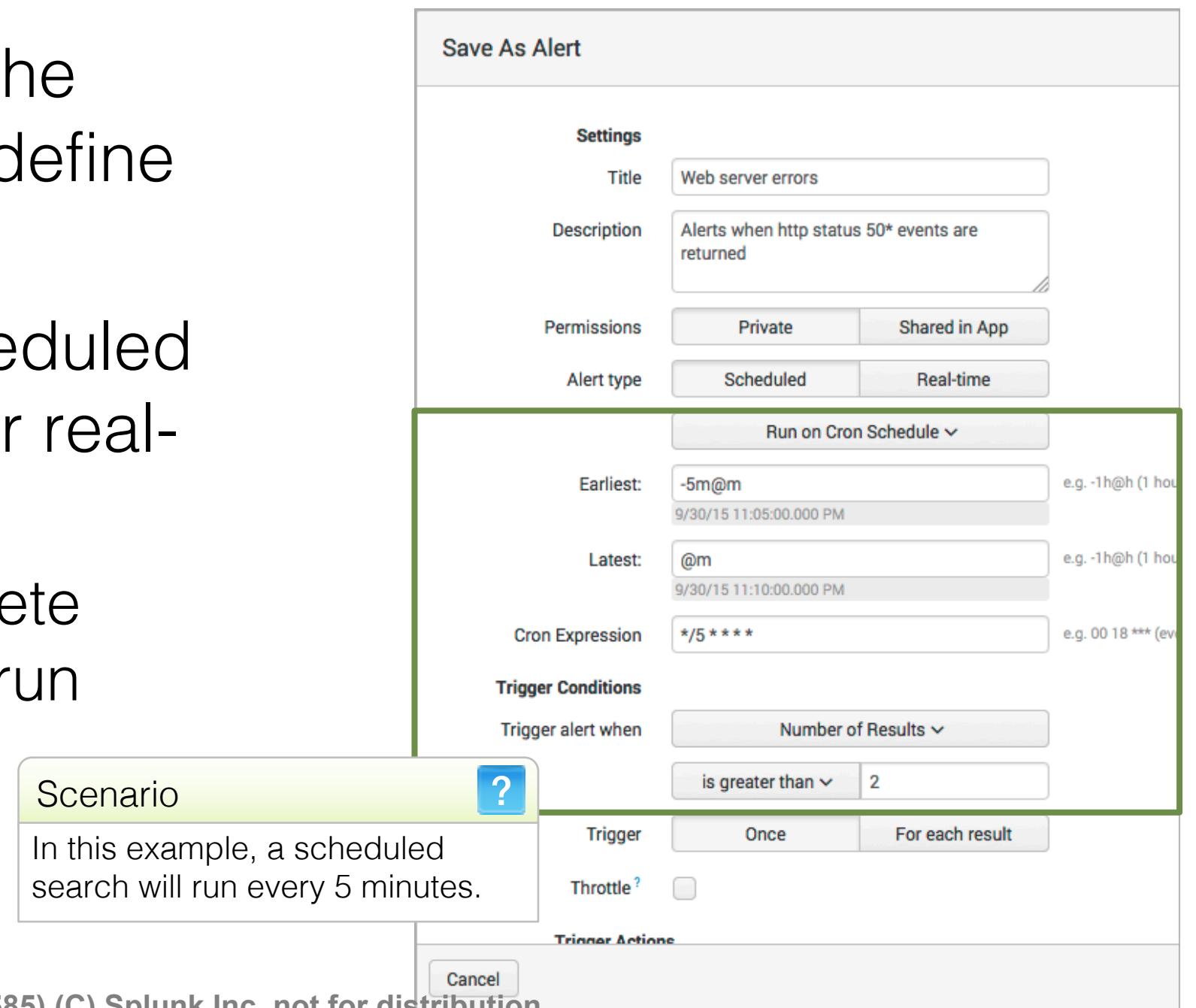
Trigger: Once | For each result

Throttle?

Scenario

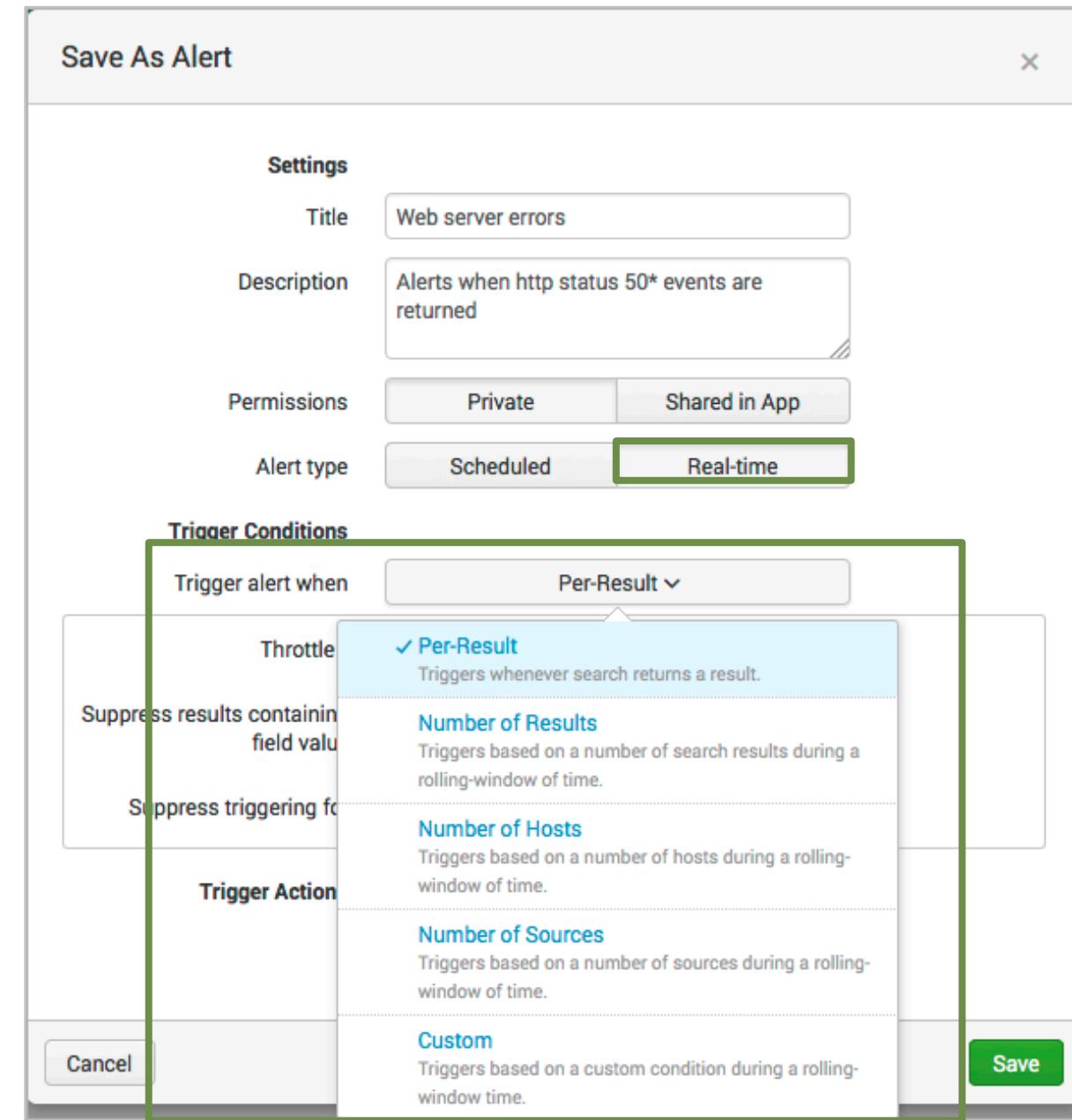
In this example, a scheduled search will run every 5 minutes.

Cancel



Setting Trigger Conditions – Real-time

- Trigger conditions allow you to capture a larger data set, then apply more stringent criteria to results before executing the alert
- You can set alerts to trigger:
 - **Per Result** – triggers when a result is returned
 - **Number of Results** – define how many results are returned before the alert triggers
 - **Number of Hosts** – define how many unique hosts are returned before the alert triggers
 - **Number of Sources** – define how many unique sources are returned before the alert triggers
 - **Custom** – define custom conditions using the search language



Setting Trigger Conditions – Real-time (cont.)

- In this example, the trigger condition is set to **Number of Results**
- In this **Real Time** alert example, if the number of results is greater than **2** within **1** minute, the alert triggers

Save As Alert x

Settings

Title	Web server errors
Description	Alerts when http status 50* events are returned
Permissions	Private Shared in App
Alert type	Scheduled Real-time

Trigger Conditions

Trigger alert when	Number of Results
is greater than	2
in	1 minute(s)
Trigger	Once For each result
Throttle?	<input type="checkbox"/>

Trigger Actions

+ Add Actions

Cancel Save

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Alert Actions – Trigger Conditions: Once

- **Once** executes actions *one time* for all matching events within the scheduled time and conditions
 - Example: If your alert is scheduled to run every 5 minutes, and 40 results are returned, the alert only triggers and executes actions one time
- Select the **Throttling** option to suppress the actions for results within a specified time range

Save As Alert

Description	Alerts when http status 50* events are returned
Permissions	Private Shared in App
Alert type	Scheduled Real-time
Run on Cron Schedule	
Earliest:	-5m@m 9/30/15 11:05:00.000 PM
Latest:	@m 9/30/15 11:10:00.000 PM
Cron Expression	*/5 * * * * e.g. 00 18 *** (every hour)
Trigger Conditions	
Trigger alert when	Number of Results
is greater than	2
Trigger	Once For each result
Throttle?	<input checked="" type="checkbox"/>
Suppress triggering for	10 minute(s)
Trigger Actions	+ Add Actions

Cancel

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Alert Actions – Trigger Conditions: For Each Result

- **For each result** – executes the alert actions once *for each result* that matches the conditions
- Select the **Throttling** option to suppress the actions for results that have the same field value, within a specified time range
 - Certain situations can cause a flood of alerts, when really you only want one
- In this example, the search runs every 5 minutes:
 - 70 events are returned in a 5 minute window
 - 50 events with status=500 and 20 include status=503
 - 2 actions will trigger, once for each status

Save As Alert

Description	Alerts when http status 50* events are returned	
Permissions	Private	Shared in App
Alert type	Scheduled	Real-time
Run on Cron Schedule ▾		
Earliest:	-5m@m 9/30/15 11:05:00.000 PM	
Latest:	@m 9/30/15 11:10:00.000 PM	
Cron Expression	*/5 * * * * e.g. 00 18 *** (eve)	
Trigger Conditions		
Trigger alert when	Number of Results ▾	
	is greater than ▾ 2	
Trigger	Once	For each result
Throttle?	<input checked="" type="checkbox"/>	
Suppress results containing field value	status	
Suppress triggering for	10	minute(s) ▾

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Add Trigger Actions

Add Actions

- **Add to Triggered Alerts** – adds the alert to the *Activity > Triggered alerts*
- **Log Event** – creates a log event to index and search
- **Run a script** – runs a script that can perform some other action
- **Send Email** – sends an email with results to recipients that you define
- **Webhook** – calls a rest endpoint using http post request

Save As Alert

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time | Run on Cron Schedule

Earliest: -5m@m | 9/30/15 11:05:00.000 PM

Latest: @m | 9/30/15 11:10:00.000 PM

Cron Expression: */5 * * * * | e.g. 00 18 *** (every hour)

Trigger Conditions

Trigger alert when: Number of Results | is greater than 2

Trigger: Once

Throttle?: checked

Suppress results containing field value: status

Suppress triggering for: 10

Trigger Actions

+ Add Actions

- Add to Triggered Alerts**
Add this alert to Triggered Alerts list
- Log Event**
Send log event to Splunk receiver endpoint
- Run a script**
Invoke a custom script
- Send email**
Send an email notification to specified recipients
- Webhook**
Generic HTTP POST to a specified URL

Alert Actions – Triggered Alerts

Choose an appropriate severity for the alert

Save As Alert

Trigger Conditions

Trigger alert when Number of Results
is greater than 0
in 1 minute(s)

Trigger Once For each result

Throttle?

Suppress results containing field value host

Suppress triggering for 60

Trigger Actions

+ Add Actions

When triggered Add to Trigger

Severity Medium

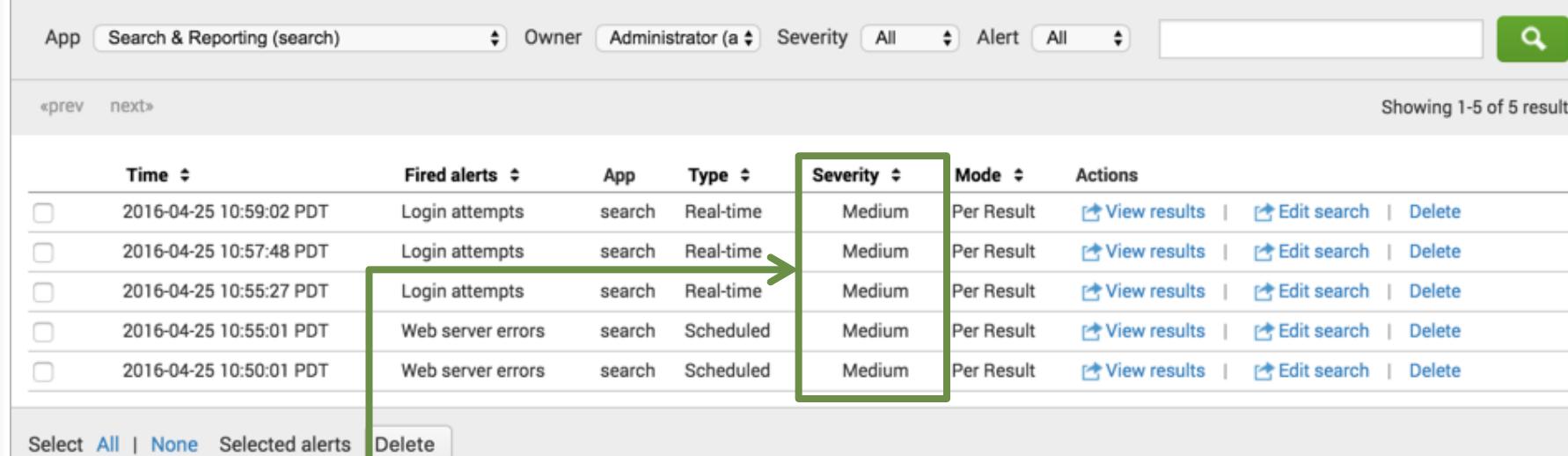


App Search & Reporting (search) Owner Administrator (a) Severity All Alert All

«prev next» Showing 1-5 of 5 results

Time	Fired alerts	App	Type	Severity	Mode	Actions
2016-04-25 10:59:02 PDT	Login attempts	search	Real-time	Medium	Per Result	View results Edit search Delete
2016-04-25 10:57:48 PDT	Login attempts	search	Real-time	Medium	Per Result	View results Edit search Delete
2016-04-25 10:55:27 PDT	Login attempts	search	Real-time	Medium	Per Result	View results Edit search Delete
2016-04-25 10:55:01 PDT	Web server errors	search	Scheduled	Medium	Per Result	View results Edit search Delete
2016-04-25 10:50:01 PDT	Web server errors	search	Scheduled	Medium	Per Result	View results Edit search Delete

Select All | None Selected alerts Delete



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Alert Actions – Log Event

If you have *administrator privileges*, you can use a log event action

- **Event** – Enter the information that will be written to the event log
- **Source** – The name of the source (alert name is used by default)
- **Sourcetype** – The name of the sourcetype used in the alert
- **Host** – The IP address of the host of the alert
- **Index** – The target index for the log event (default value is main)

When triggered

Log Event

Remove

Event

\$trigger_date\$ \$trigger_timeHMS\$ 50* web server errors sourcetype=\$result.sourcetype\$

Specify event text for the logged event.
[Learn More](#)

Source

alert:\$name\$

Value of the source field.

Sourcetype

access_combined

Value of the sourcetype field.

Host

Value of the host field.

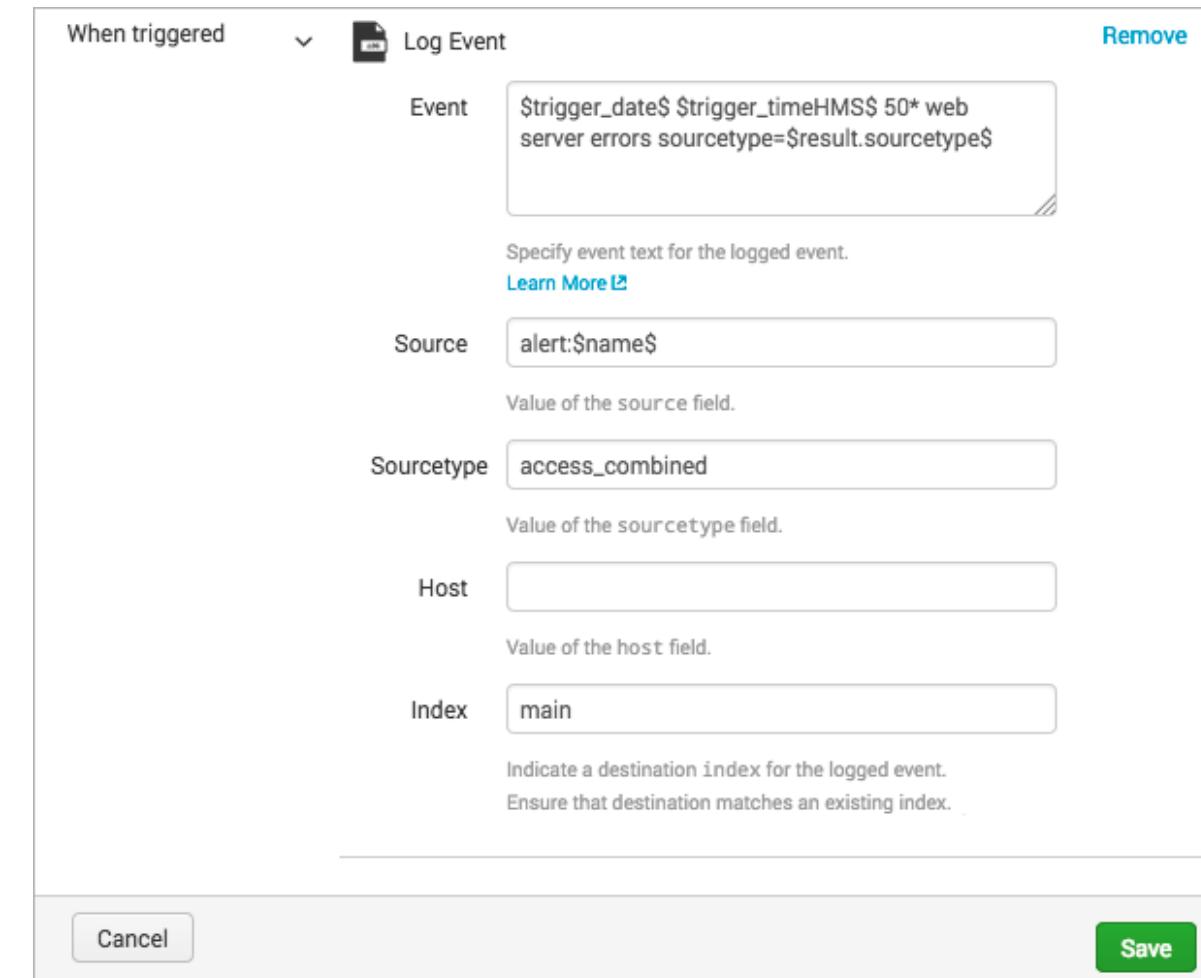
Index

main

Indicate a destination index for the logged event.
Ensure that destination matches an existing index.

Cancel

Save



Note

For a complete list of available tokens, go to:
<http://docs.splunk.com/Documentation/Splunk/latest/Alert/EmailNotificationTokens>

Alert Actions – Log Event (cont.)

The screenshot shows the Splunk Alert Actions interface for a 'Log Event' action. On the left, the 'Event' field contains the template: '\$trigger_date\$ \$trigger_timeHMS\$ 50* web server errors sourcetype=\$result.sourcetype\$'. Below it, the 'Source' field is set to 'alert:\$name\$', 'Sourcetype' is 'access_combined', and 'Host' is empty. The 'Index' field is set to 'main'. A yellow box highlights the 'Source', 'Sourcetype', and 'Index' fields. A red box highlights the 'Host' field. A blue arrow points from the 'Source' field in the alert configuration to the 'source' field in the search results table. Another blue arrow points from the 'Sourcetype' field in the alert configuration to the 'sourcetype' field in the search results table. A green box highlights the first event in the search results table.

Time	Event
2016-08-18 22:51:55 50*	host = 127.0.0.1 source = alert:LogEvent sourcetype = access_combined
2016-08-18 22:51:53 50*	host = 127.0.0.1 source = alert:LogEvent sourcetype = access_combined
2016-08-18 22:51:50 50*	host = 127.0.0.1 source = alert:LogEvent sourcetype = access_combined

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Alert Actions – Send Email

Customize the content of email alerts

- **To** - enter the email address(es) of the alert recipients
- **Priority** – select the priority
- **Subject** – edit the subject of the email (the \$name\$ token is the title of the alert)
- **Message** – provide the message body of the email
- **Include** - select the format of the alert
- **Type** – select the format of the text message

Save As Alert

+ Add Actions ▾

When triggered

Send email

Remove

To

Priority

Normal

Subject

Splunk Alert: \$name\$

Message

The alert condition for '\$name\$' was triggered.

Comma separated list of email addresses.
Show CC and BCC

The email subject and message can include tokens that insert text based on the results of the search. [Learn More](#)

Include

Link to Alert Link to Results
 Search String Inline [Table](#) ▾
 Trigger Condition Attach CSV
 Trigger Time Attach PDF

Type

[HTML & Plain Text](#) [Plain Text](#)

Cancel

Save

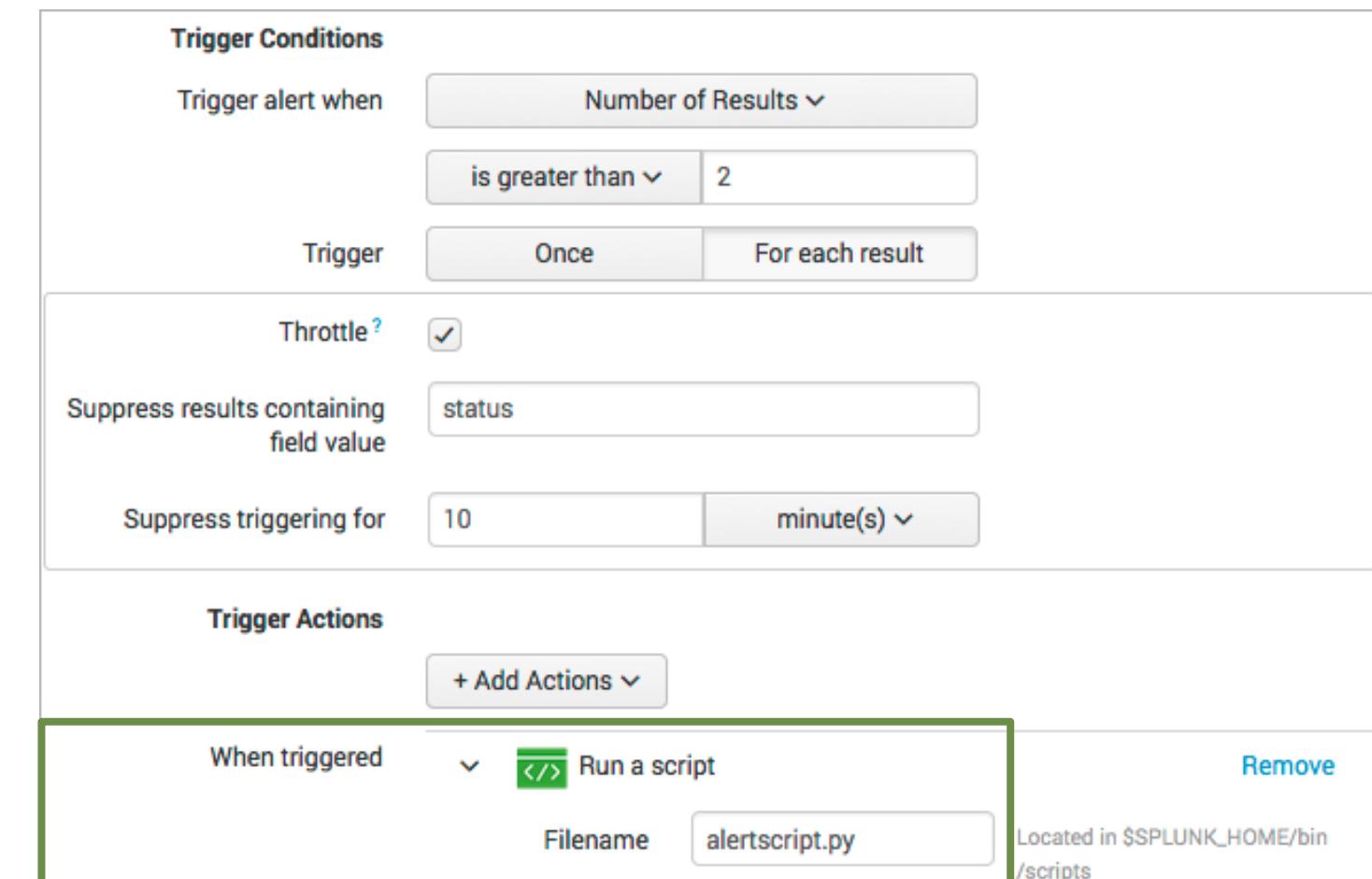
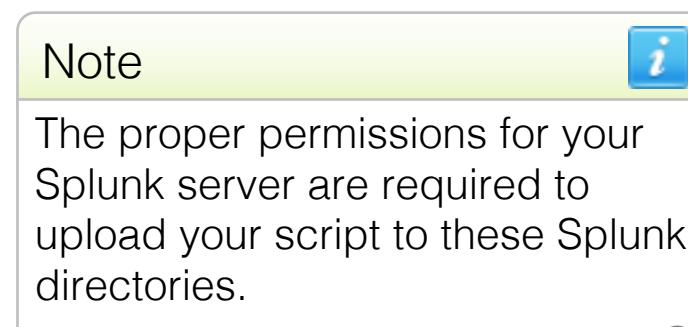
Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Alert Actions – Run a Script

- When an alert is triggered, you can launch a script
 - Enter the name of the script
 - All alert scripts need to reside in either of the following locations:

\$SPLUNK_HOME/bin/scripts

**\$SPLUNK_HOME/etc/apps/
<Appname>/bin/scripts**



The screenshot shows the 'Trigger Conditions' section with the following settings:

- Trigger alert when: Number of Results > 2
- Trigger: Once
- Throttle: checked
- Suppress results containing field value: status
- Suppress triggering for: 10 minute(s)

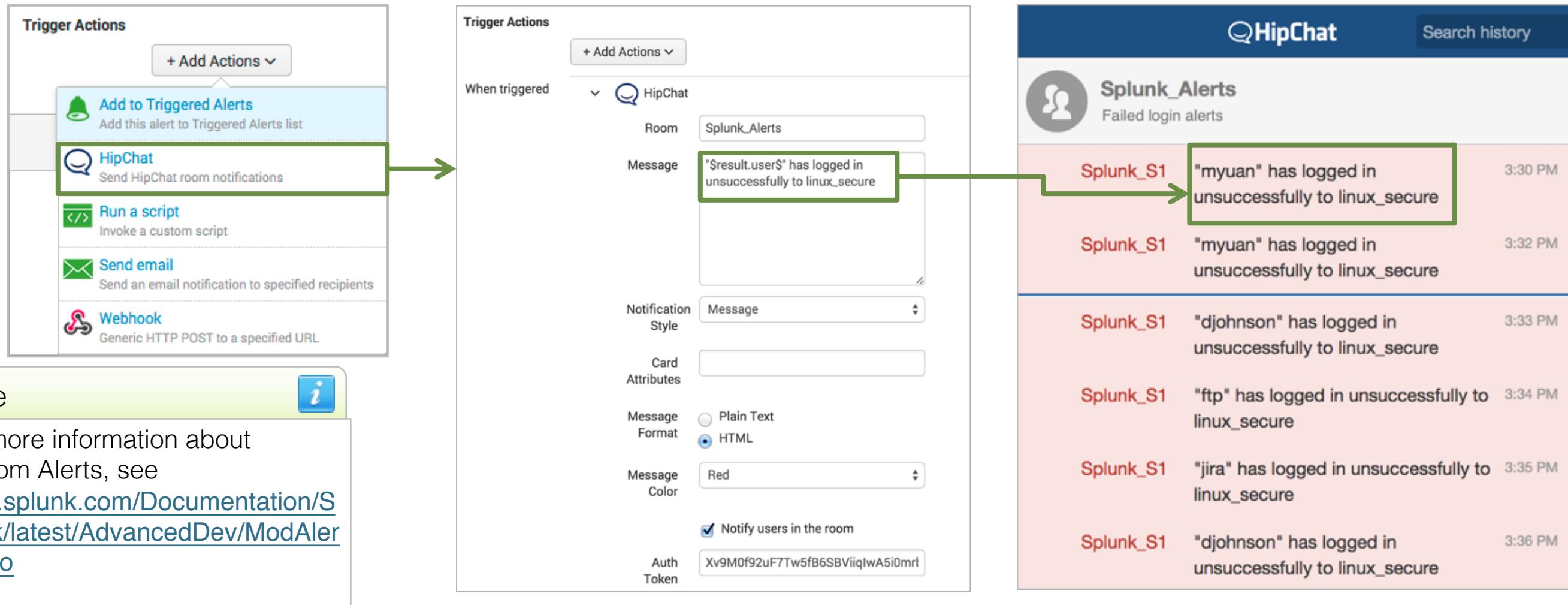
The 'Trigger Actions' section contains a single action:

- + Add Actions
- When triggered: Run a script
- Filename: alertscript.py

A green box highlights the 'Run a script' action. A note at the bottom right says 'Located in \$SPLUNK_HOME/bin/scripts'.

Custom Alert Action - Example

- A custom alert action can be created or an admin can install and configure app from Splunkbase
- In this example, the HipChat Room Notification Alert app is used



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Viewing Triggered Alerts

- If you elected to list in triggered alerts, you can view the results by accessing **Activity > Triggered Alerts**
- Click **View results** to see the matching events that triggered the alert
- Click **Edit search** to modify the alert definition

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

- Header:** splunk> Apps ▾ cfarrell ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find
- Search Bar:** App: Search & Reporting (search), Owner: cfarrell (cfarrell), Severity: All, Alert: All.
- Filter:** Jobs (highlighted in blue) and Triggered Alerts (highlighted in green).
- Table Headers:** Time, Fired alerts, App, Type, Severity, Mode, Actions.
- Table Data:**

Time	Fired alerts	App	Type	Severity	Mode	Actions
2016-08-18 16:42:32 PDT	Failed login attempts	search	Real-time	High	Digest	View results Edit search Delete
2016-08-18 16:37:58 PDT	Failed login attempts	search	Real-time	High	Per Result	View results Edit search Delete
2016-08-18 16:20:37 PDT	Web server errors	search	Real-time	Medium	Per Result	View results Edit search Delete
- Page Information:** Showing 1-3 of 3 results.

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Editing Alerts

1. From the search bar, click **Alerts**
2. Select the alert and click **Edit**

The screenshot shows the Splunk interface with the 'Search & Reporting' tab selected. In the top navigation bar, the 'Alerts' tab is also selected. The main content area displays the 'Alerts' page. There are two alerts listed:

i	Title ^	Actions	Owner	App	Sharing
>	Failed login attempts by user admin	Open in Search Edit	cfarrell	search	App
>	Web server errors	Open in Search Edit	cfarrell	search	App

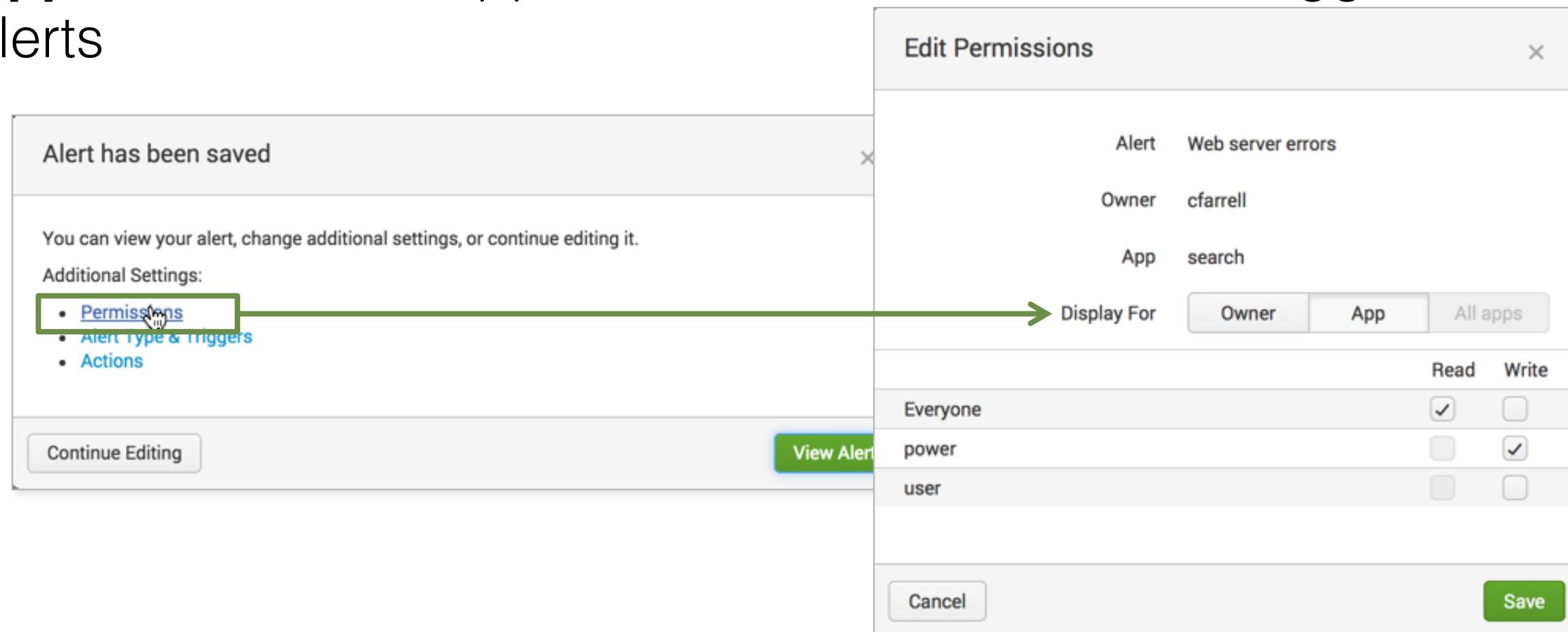
A green box highlights the 'Edit' button for the 'Web server errors' alert. An arrow points from this highlighted button to a context menu that appears over the row. The context menu contains the following options:

- Edit Description
- Edit Permissions
- Edit Alert Type and Trigger Condition
- Edit Actions
- Disable
- Clone
- Delete

Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Editing Alert Permissions

- Edit permissions
 - **Owner** – only you can access, edit, and view triggered alerts
 - **App** – users of the app can access, edit, and view triggered alerts



Generated for Anil Gogia (6756585) (C) Splunk Inc, not for distribution

Support Programs

- **Community**

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

- **Global Support**

Support for critical issues, a dedicated resource to manage your account – 24 x 7 x 365.

- **Phone: (855) SPLUNK-S or (855) 775-8657**
- **Web:** http://www.splunk.com/index.php/submit_issue

- **Enterprise Support**

Access your customer support team by phone and manage your cases online 24 x 7
(depending on support contract.)