



# Splunk Fundamentals 1

Generated for () (C) Splunk Inc, not for distribution

# Outline

---

Module 1: Introducing Splunk

Module 2: Splunk Components

Module 3: Installing Splunk

Module 4: Getting Data In

Module 5: Basic Search

Module 6: Using Fields

Module 7: Best Practices

Module 8: Splunk's Search Language

Module 9: Transforming Commands

Module 10: Creating Reports and Dashboards

Module 11: Pivot and Datasets

Module 12: Creating and Using Lookups

Module 13: Creating Scheduled Reports and Alerts

Generated for () (C) Splunk Inc, not for distribution

# Module 1

# Introducing Splunk

Generated for () (C) Splunk Inc, not for distribution

# Understanding Splunk

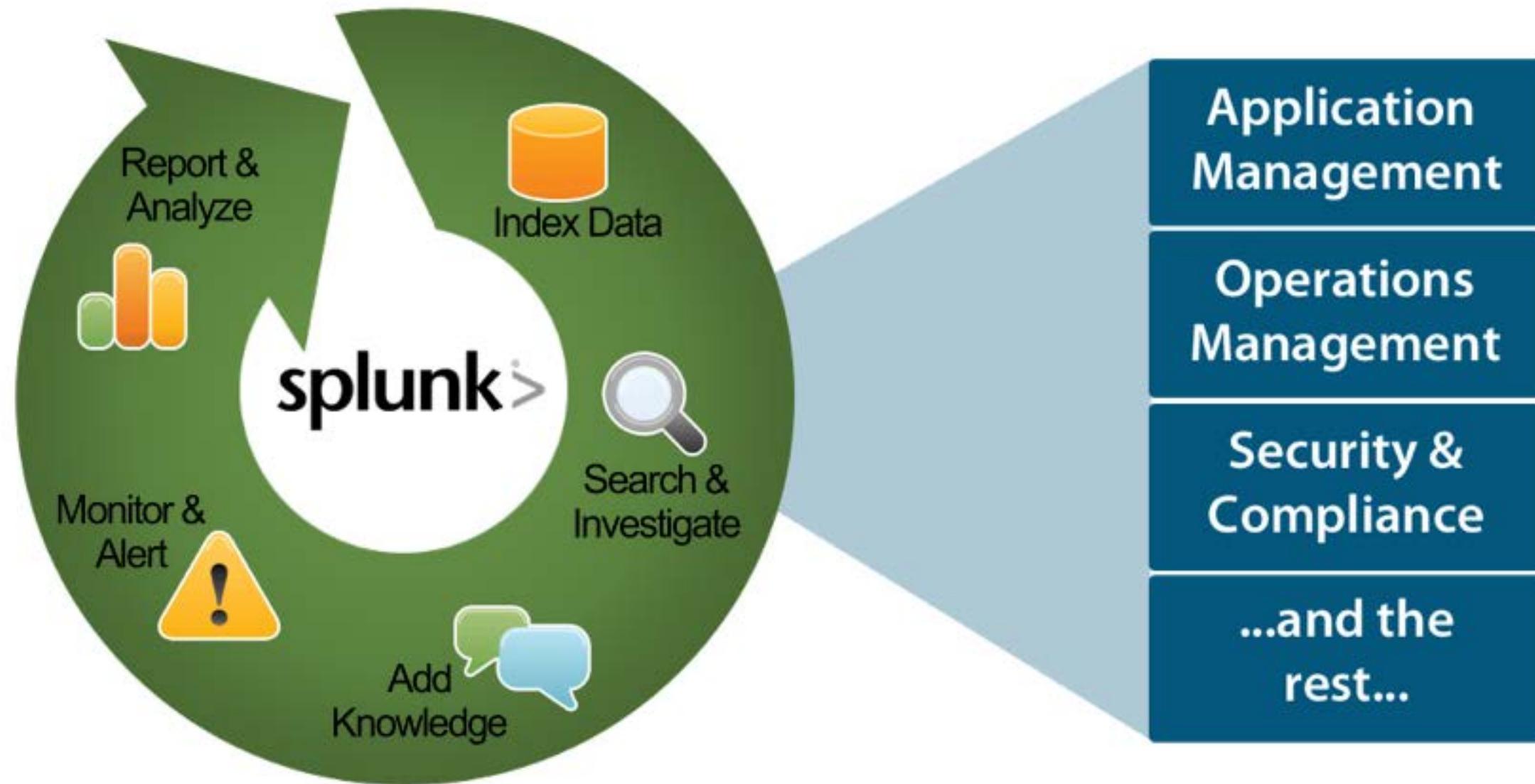
---



- What Is Splunk?
- What Data?
- How Does Splunk Work?
- How Is Splunk Deployed?
- What are Splunk Apps?
- What are Splunk Enhanced Solutions?

Generated for () (C) Splunk Inc, not for distribution

# What Is Splunk?



Aggregate, analyze, and get answers from your machine data

Generated for () (C) Splunk Inc, not for distribution

# What Data?

## Index ANY data from ANY source



- Computers
- Network devices
- Virtual machines
- Internet devices
- Communication devices
- Sensors
- Databases

Note

For lots of ideas on data to collect in your environment, get the Splunk publication [The Essential Guide to Machine Data](#).



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

# How Does Splunk Work?

Splunk  
Search Head



Splunk  
Indexer



Splunk Forwarders

Generated for (c) Splunk Inc, not for distribution

# How Is Splunk Deployed?

- **Splunk Enterprise**

- Splunk components installed and administered on-premises



- **Splunk Cloud**

- Splunk Enterprise as a scalable service
  - No infrastructure required



- **Splunk Light**

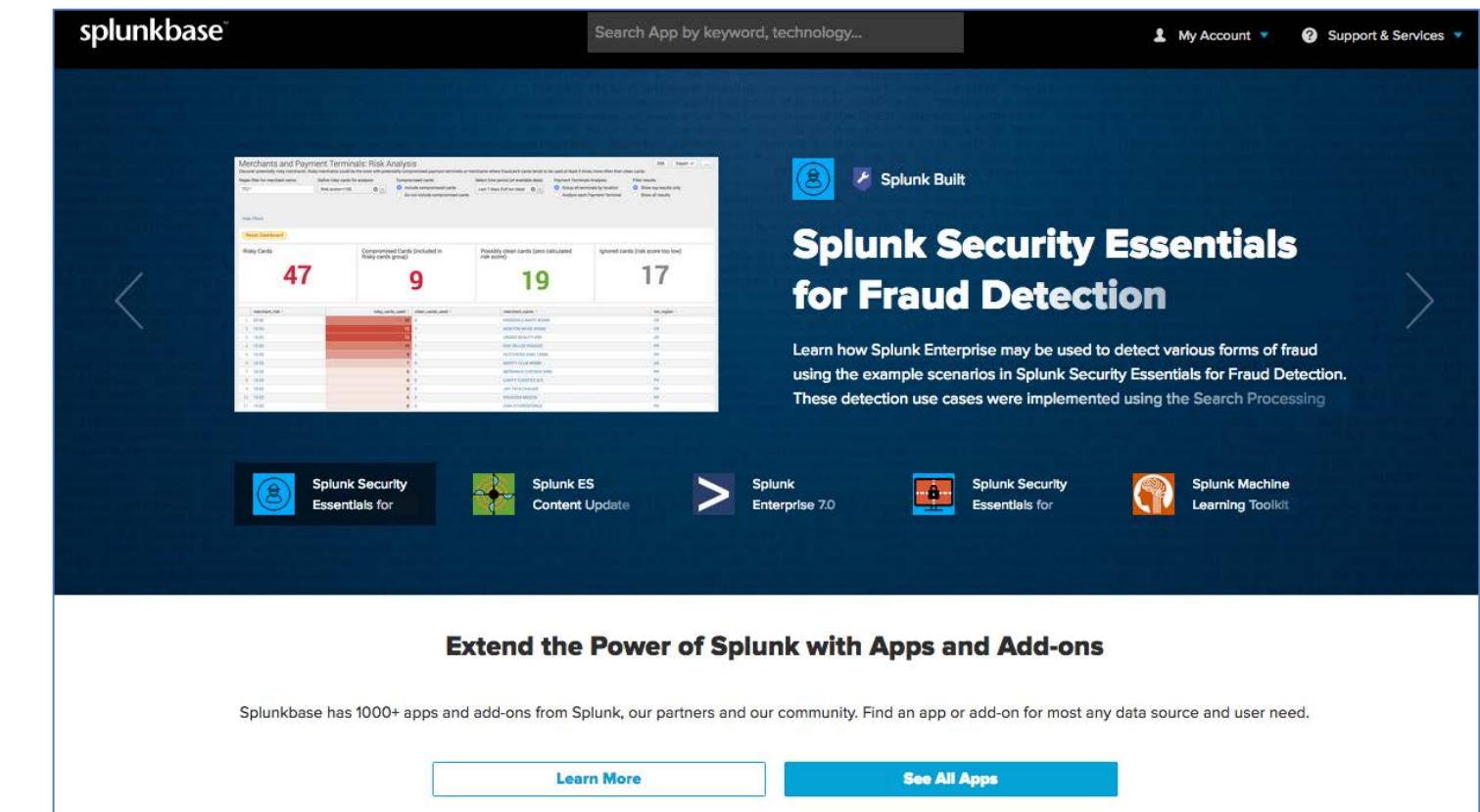
- Solution for small IT environments



Generated for () (C) Splunk Inc, not for distribution

# What are Splunk Apps?

- Designed to address a wide variety of use cases and to extend the power of Splunk
- Collections of files containing data inputs, UI elements, and/or knowledge objects
- Allows multiple workspaces for different use cases/user roles to co-exist on a single Splunk instance
- 1000+ ready-made apps available on Splunkbase ([splunkbase.com](https://splunkbase.com)) or admins can build their own



Generated for () (C) Splunk Inc, not for distribution

# What are Splunk Enhanced Solutions?

- **Splunk IT Service Intelligence (ITSI)**

- Next generation monitoring and analytics solution for IT Ops
  - Uses machine learning and event analytics to simplify operations and prioritize problem resolution



- **Splunk Enterprise Security (ES)**

- Comprehensive Security Information and Event Management (SIEM) solution
  - Quickly detect and respond to internal and external attacks



- **Splunk User Behavior Analytics (UBA)**

Finds known, unknown, and hidden threats by analyzing user behavior and flagging unusual activity



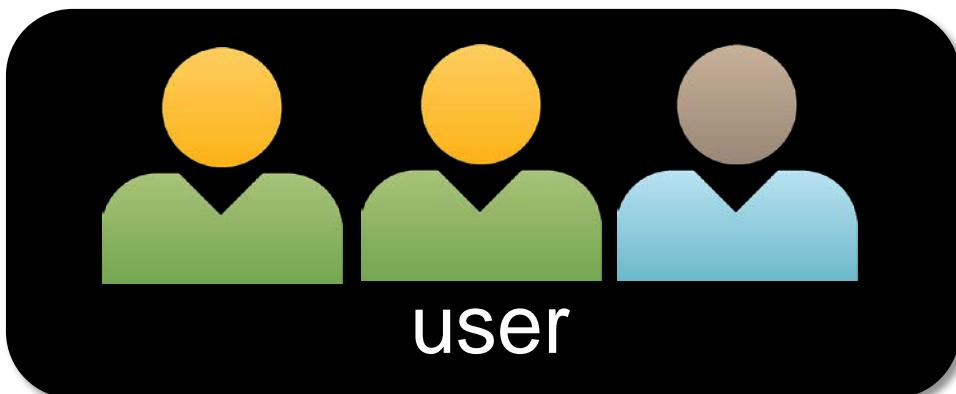
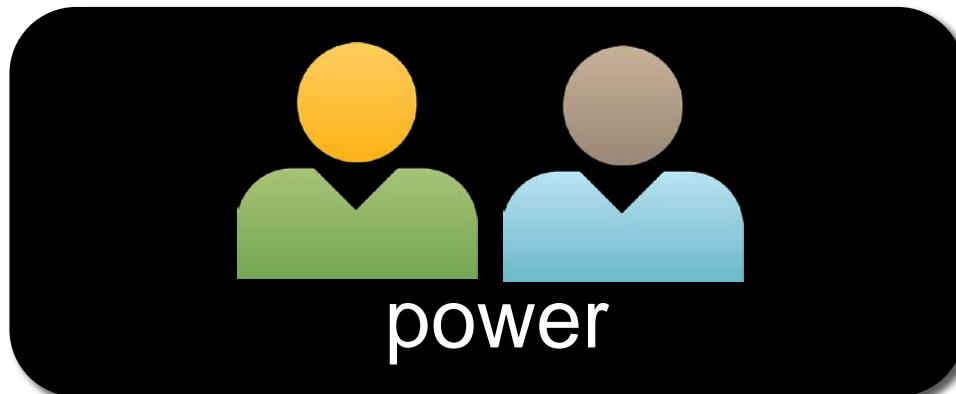
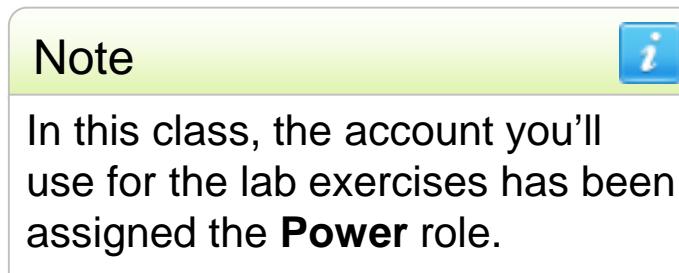
Note

For more info, see Appendix A:  
Splunk Premium Solutions and Apps.

Generated for () (C) Splunk Inc, not for distribution

# Users and Roles

- Splunk users are assigned roles, which determine their capabilities and data access
- Out of the box, there are 3 main roles:
  - Admin
  - Power
  - User
- Splunk admins can create additional roles



Generated for () (C) Splunk Inc, not for distribution

# Logging In

- 1 Log into Splunk with a web browser
- 2 The main view of your default app appears

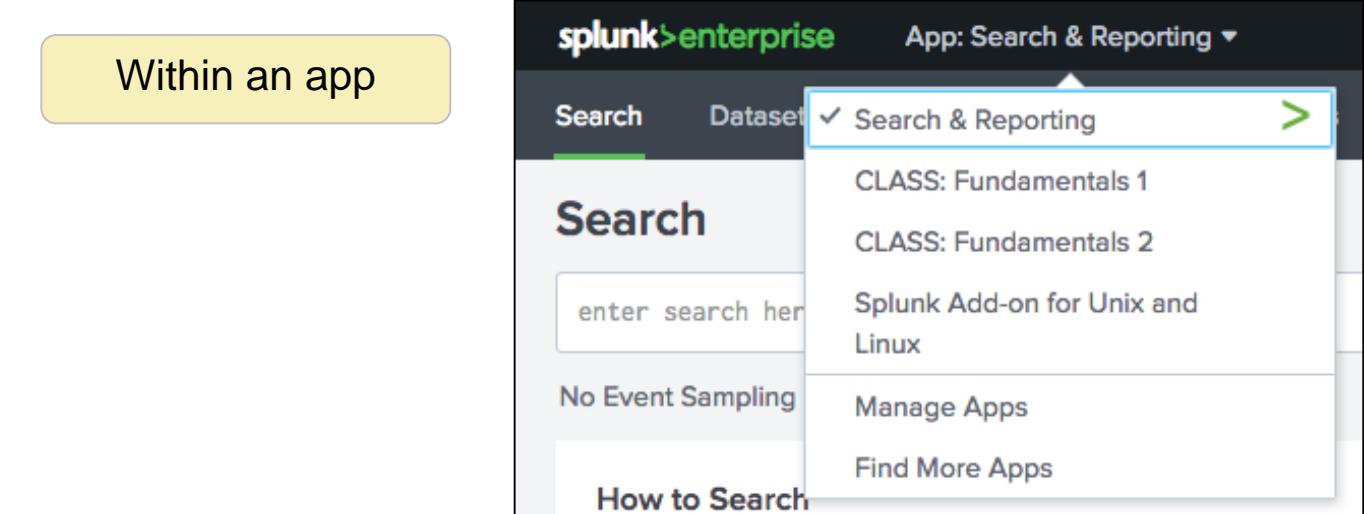
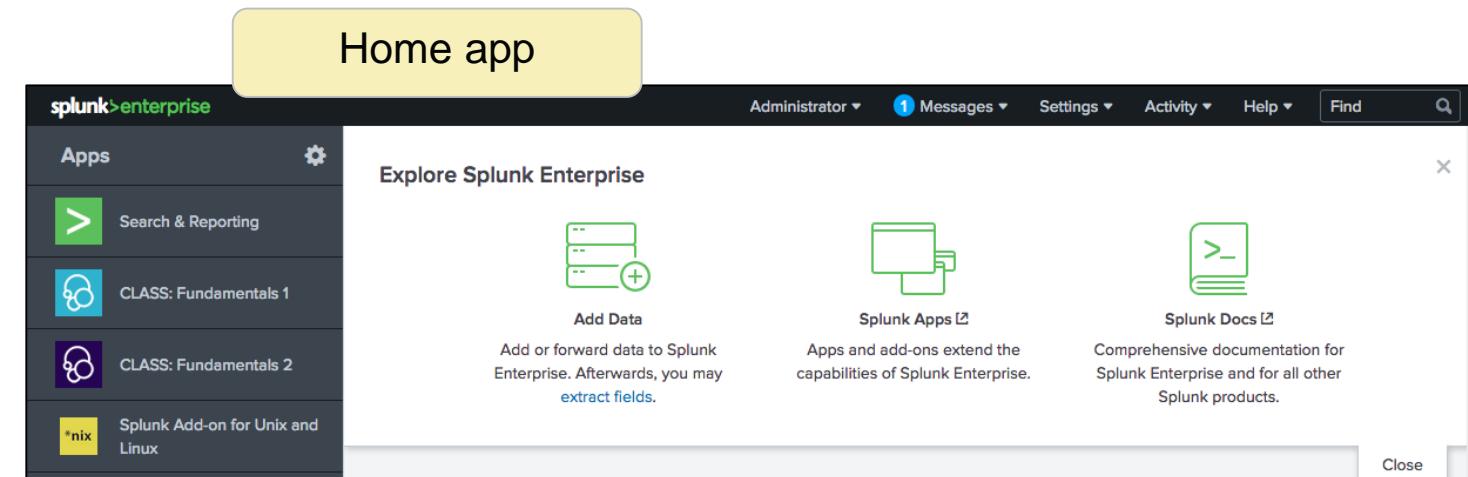
You or your organization may change your default app



A screenshot of the Splunk Enterprise search interface. The top navigation bar includes the "splunk&gt;enterprise" logo, a dropdown for "App: Search &amp; Reporting", user information (student1), and various settings. A red circle with the number "2" highlights the "Search" tab in the navigation bar. The main area shows a search bar with "enter search here...", a time range selector set to "Last 24 hours", and a "Search &amp; Reporting" button. On the left, there's a "How to Search" section with links to "Documentation" and "Tutorial". On the right, there's a "What to Search" summary showing "5,981,905 Events" from "7 months ago" to "Now", with links to "INDEXED", "EARLIEST EVENT", and "LATEST EVENT". At the bottom, it says "Generated for () (C) Splunk Inc, not for distribution".

# Choosing Your App

- Apps allow different workspaces for specific use cases or user roles to co-exist on a single Splunk instance
- In this class, you'll explore:
  - The Home app
  - The Search & Reporting app (also called the Search app)



## Note

For more info on apps, see.  
<http://docs.splunk.com/Documentation/Splunk/latest/Admin/Whatsanapp>



# Home App

You can always click the Splunk logo to return to whatever app is set as your default app.

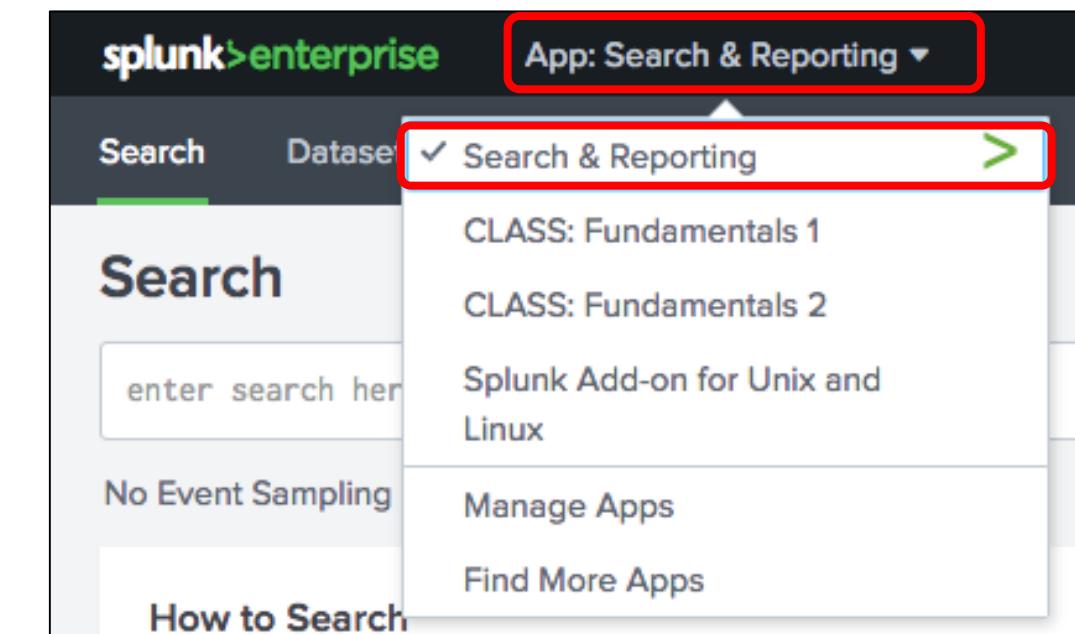
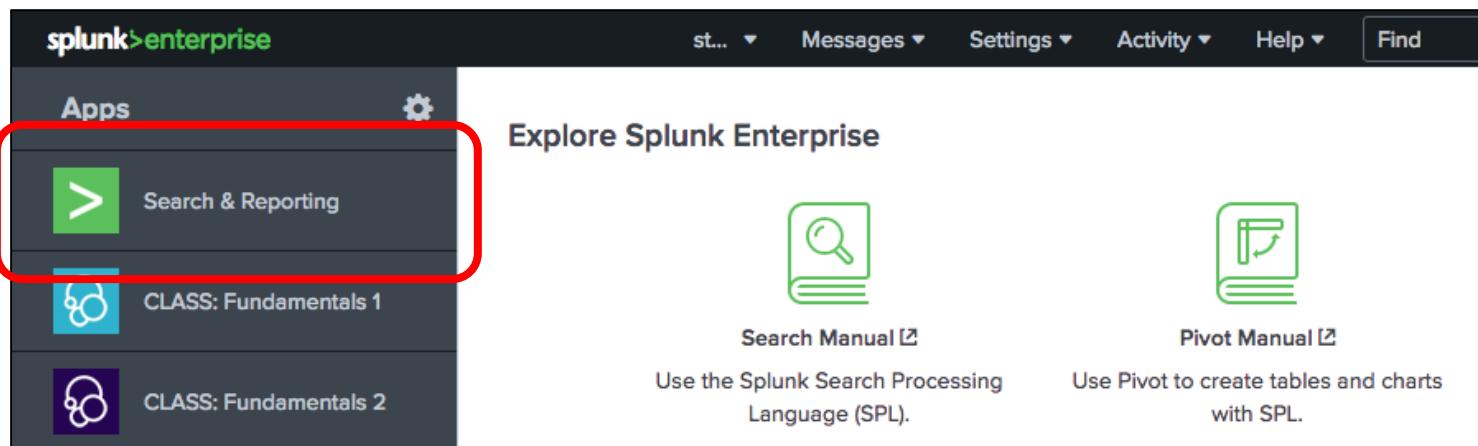
The screenshot shows the Splunk Enterprise Home App interface. At the top, there's a navigation bar with 'student1' (dropdown), 'Messages' (dropdown), 'Settings' (dropdown), 'Activity' (dropdown), 'Help' (dropdown), 'Find', and a search icon. Below the navigation bar is the 'splunk>enterprise' logo. To the right of the logo is a yellow callout box containing the text 'Links to several helpful resources'. On the left side, there's a sidebar titled 'Apps' with a gear icon. It lists four items: 'Search & Reporting' (green icon), 'CLASS: Fundamentals 1' (blue icon), 'CLASS: Fundamentals 2' (purple icon), and 'Splunk Add-on for Unix and Linux' (yellow icon). At the bottom left, there's a 'Note' section with an info icon, containing the text: 'If you or your organization doesn't choose a default app, then your default app is the Home app.' To the right of the sidebar is a main content area titled 'Explore Splunk Enterprise'. It features three cards: 'Search Manual' (with a magnifying glass icon), 'Pivot Manual' (with a chart icon), and 'Dashboards & Visualizations' (with a dashboard icon). Below these cards is a section titled 'Choose a home dashboard' with a monitor icon.

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

Generated for () (C) Splunk Inc, not for distribution

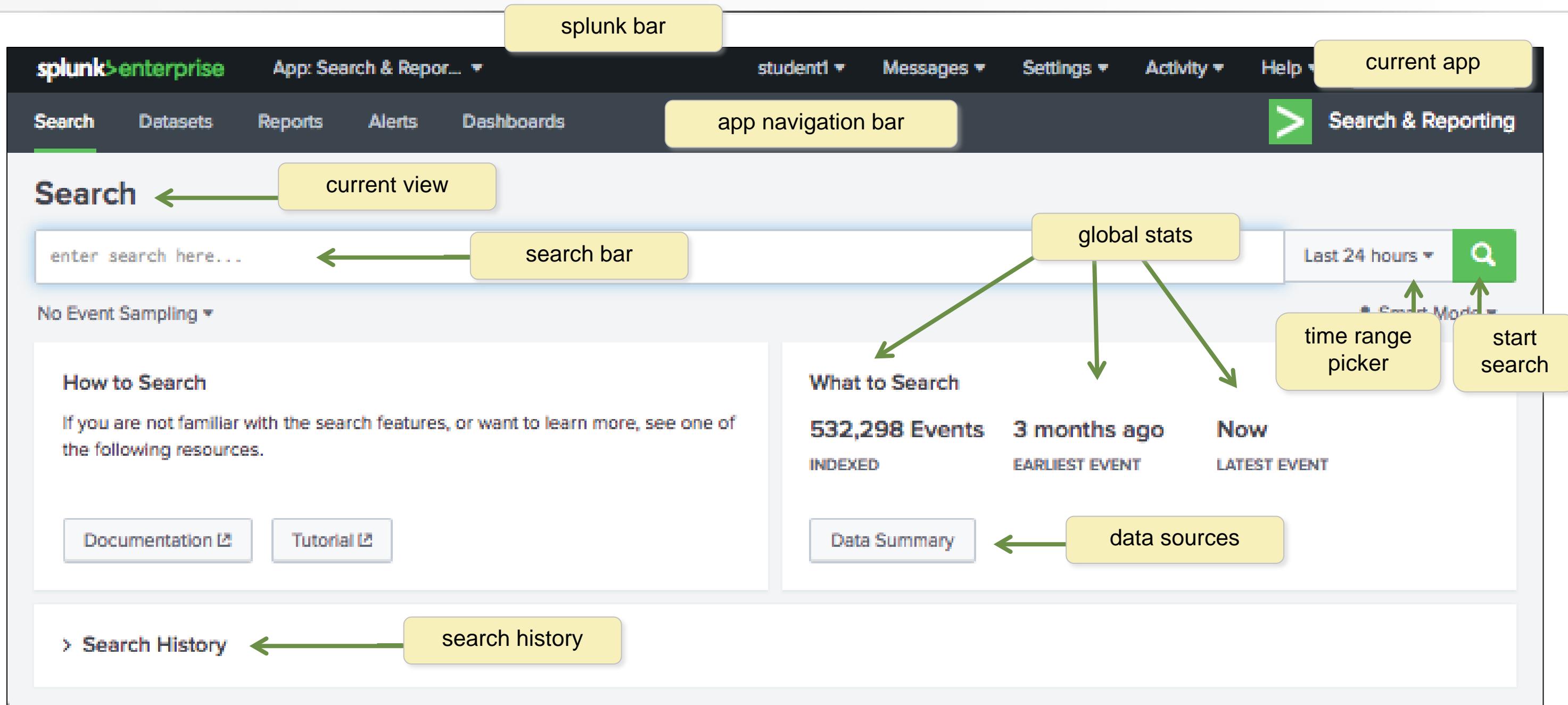
# Search & Reporting App

- 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 app or from an app view, select **Apps > Search & Reporting**



Generated for () (C) Splunk Inc, not for distribution

# Search & Reporting App (cont.)



Generated for () (C) Splunk Inc, not for distribution

# Data Summary Tabs

The screenshot shows the Splunk Enterprise search interface. At the top, there's a navigation bar with links for Search, Datasets, Reports, Alerts, and Dashboards. Below the navigation bar is a search bar with a placeholder 'enter search here...' and a time range selector 'Last 24 hours'. To the right of the search bar is a yellow callout box with the text: 'Click Data Summary to see hosts, sources, or sourcetypes on separate tabs'. The main area is titled 'Data Summary' and contains three tabs: 'Hosts (10)', 'Sources (15)', and 'Sourcetypes (10)'. Each tab has a 'filter' button and a list of items. A green arrow points from the 'Data Summary' button in the 'What to Search' section of the main interface to the 'Hosts (10)' tab. Another green arrow points from the 'Sources (15)' tab to a yellow callout box containing the text: 'Tables can be sorted or filtered'. A third green arrow points from the 'Sourcetypes (10)' tab to the same yellow callout box.

- Host – Unique identifier of where the events originated (host name, IP address, etc.)
- Source - Name of the file, stream, or other input
- Sourcetype - Specific data type or data format

| Sourcetype                 | Count   | Last Update            |
|----------------------------|---------|------------------------|
| SimCubeBeta                | 377     | 1/4/18 3:51:45.000 PM  |
| access_combined            | 154,373 | 1/4/18 3:52:18.000 PM  |
| cisco_esa                  | 3,200   | 1/4/18 3:52:15.000 PM  |
| cisco_firewall             | 538     | 1/4/18 10:23:47.000 AM |
| cisco_wsa_squid            | 3,749   | 1/4/18 3:50:37.000 PM  |
| history_access             | 7,662   | 1/4/18 10:23:46.000 AM |
| linux_secure               | 16,950  | 1/4/18 3:52:12.000 PM  |
| sales_entries              | 215,869 | 1/4/18 3:51:56.000 PM  |
| vendor_sales               | 120,459 | 1/4/18 3:49:32.000 PM  |
| winauthentication_security | 9,372   | 1/4/18 10:23:46.000 AM |

Generated for () (C) Splunk Inc, not for distribution

# Events Tab

The screenshot shows the Splunk Enterprise interface with the 'Search & Reporting' app selected. A search query 'error OR fail\*' is entered in the search bar, resulting in 2,044 events found over the last 24 hours. The 'Events (2,044)' tab is selected, displaying a timeline of events from January 4, 2018, at 16:12:44. The events list includes fields such as host, source, and sourcetype. Two specific events are highlighted with yellow boxes: one for a failed password attempt from user 'informix' and another for a failed password attempt from user 'admin'. The 'event' field is also highlighted in yellow.

| Time                  | Event  |
|-----------------------|--|
| 1/4/18 4:12:44.000 PM | Thu Jan 04 2018 16:12:44 www2 sshd[1967]: Failed password for invalid user informix from 10.3.10.4 port 4696 ssh2<br>host = www2   source = /opt/log/www2/secure.log   sourcetype = linux_secure |
| 1/4/18 4:12:39.000 PM | Thu Jan 04 2018 16:12:39 www2 sshd[5138]: Failed password for invalid user info from 10.3.10.46 port 2997 ssh2<br>host = www2   source = /opt/log/www2/secure.log   sourcetype = linux_secure    |
| 1/4/18 4:12:33.000 PM | Thu Jan 04 2018 16:12:33 www2 sshd[5909]: Failed password for gopher from 10.3.10.46 port 1548 ssh2<br>host = www2   source = /opt/log/www2/secure.log   sourcetype = linux_secure               |
| 1/4/18 4:12:23.000 PM | Thu Jan 04 2018 16:12:23 www2 sshd[2459]: Failed password for invalid user admin from 10.3.10.46 port 2645 ssh2<br>host = www2   source = /opt/log/www2/secure.log   sourcetype = linux_secure   |

Generated for () (C) Splunk Inc, not for distribution

# Course Scenario

- Use cases in this course are based on Buttercup Games, a fictitious gaming company
- Multinational company with its HQ in San Francisco and offices in Boston and London
- Sells products through its worldwide chain of 3<sup>rd</sup> party stores and through its online store



Generated for () (C) Splunk Inc, not for distribution

# Your Role at Buttercup Games

---

- You're a Splunk power user
- You're responsible for providing info to users throughout the company
- You gather data/statistics and create reports on:
  - IT operations: information from mail and internal network data
  - Security operations: information from internal network and badge reader data
  - Business analytics: information from web access logs and vendor data

# Callouts

## Scenarios

- Many of the examples in this course relate to a specific scenario
- For each example, a question is posed from a colleague or manager at Buttercup Games

### Scenario



For failed logins into the network during the last 60 minutes, display the IP and user name.

## Notes & Tips

References for more information on a topic and tips for best practices

### Note



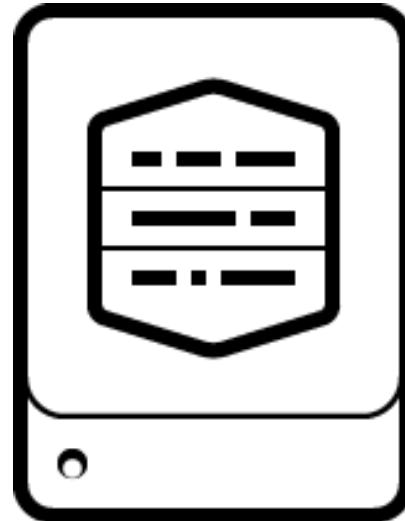
Learn more about Splunk from Splunk's online glossary, the Splexicon at <http://docs.splunk.com/Splexicon>

# Module 2: Splunk Components

Generated for () (C) Splunk Inc, not for distribution

# Splunk Components

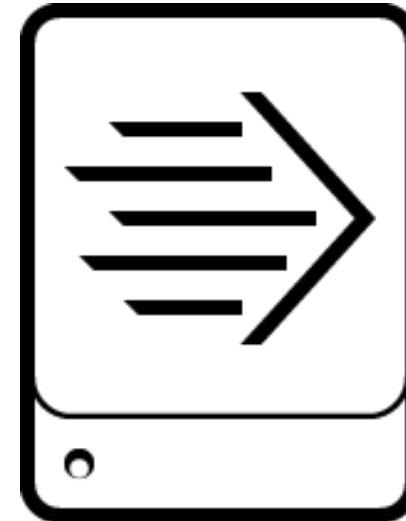
Splunk is comprised of three main processing components:



**Indexer**



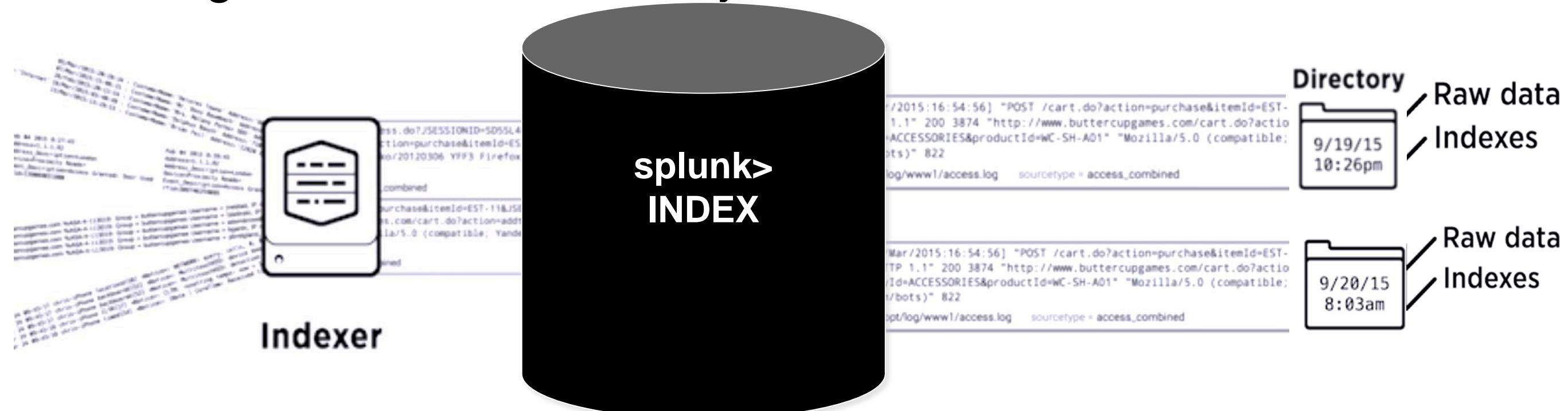
**Search Head**



**Forwarder**

# Splunk Components - Indexer

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

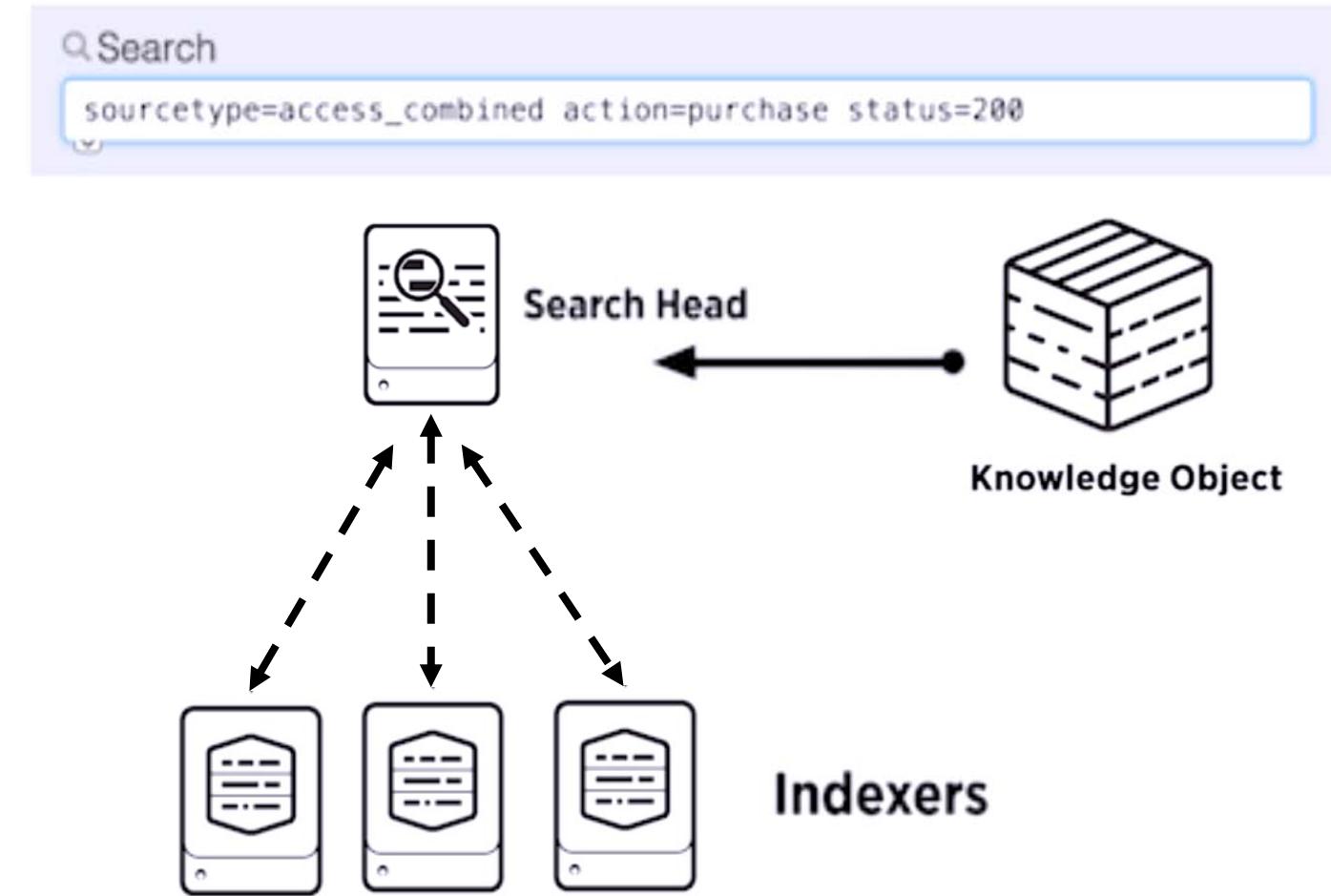


- As the Indexer indexes data, it creates a number of files organized in sets of directories by age
  - Contains raw data (compressed) and indexes (points to the raw data)

Generated for () (C) Splunk Inc, not for distribution

# Splunk Components – Search Heads

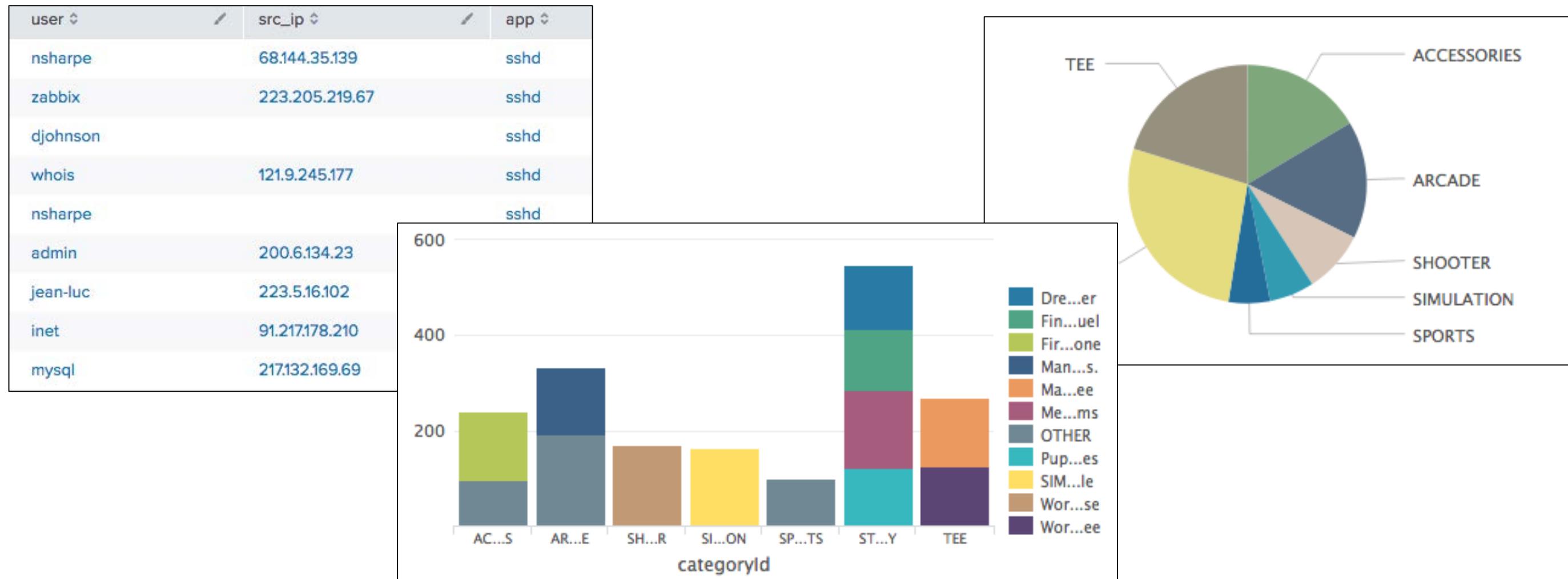
- Allows users to use the Search language to search the indexed data
- Distributes user search requests to the Indexers
- Consolidates the results and extracts field value pairs from the events to the user
- Knowledge Objects on the Search Heads can be created to extract additional fields and transform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



Generated for () (C) Splunk Inc, not for distribution

# Splunk Components – Search Heads (cont.)

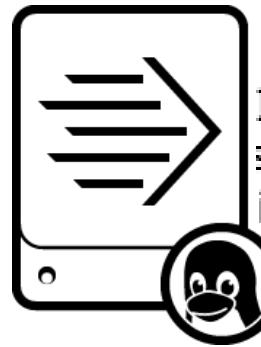
Search Heads also provide tools to enhance the search experience such as reports, dashboards and visualizations



Generated for () (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 = TPsecOverTLS, IP = 10.1.10.216, Session connected. Session type = SSL, Duration = 10.1.10.216, IP = 10.1.10.133, Session connected. Session type = IKE, Duration = 10.1.10.133, IP = 10.3.10.18, Session disconnected. Session type = IKE, Duration = 10.3.10.18, IP = 10.1.10.211, Session connected. Session type = SSL, Duration = 10.1.10.211

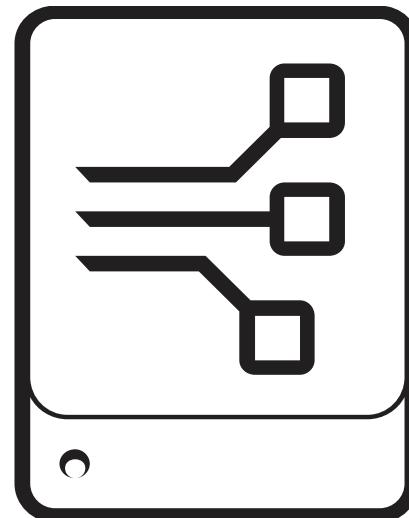


Indexer

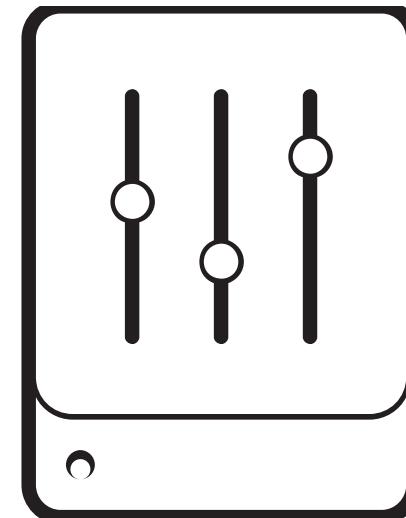
Generated for () (C) Splunk Inc, not for distribution

# Additional Splunk Components

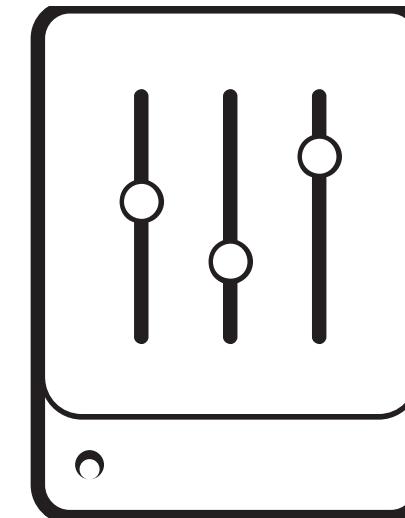
In addition to the three main Splunk processing components, there are some less-common components including :



**Deployment  
Server**



**Cluster Master**

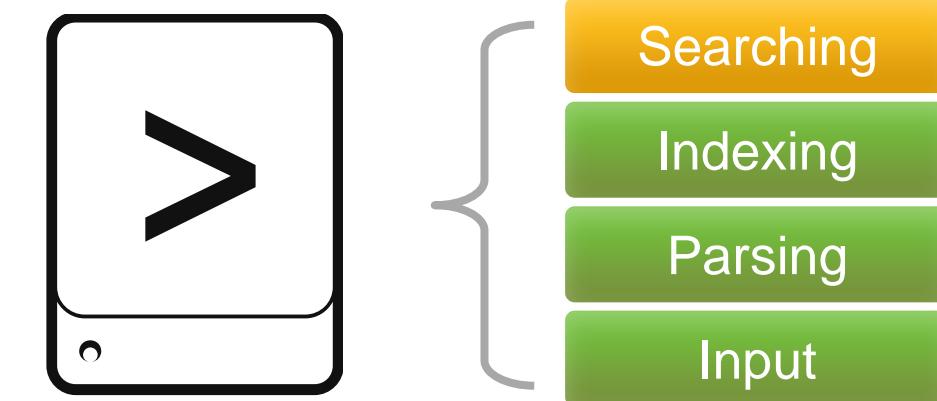


**License Master**

# 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



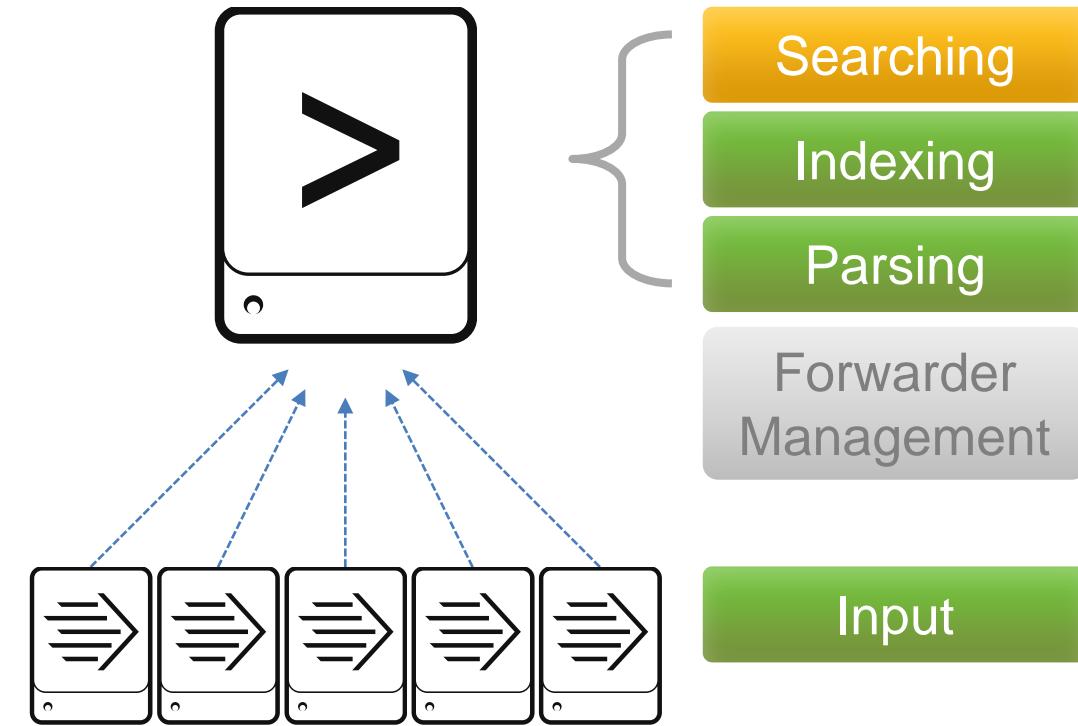
- Recommendation

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

Generated for () (C) Splunk Inc, not for distribution

# 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)

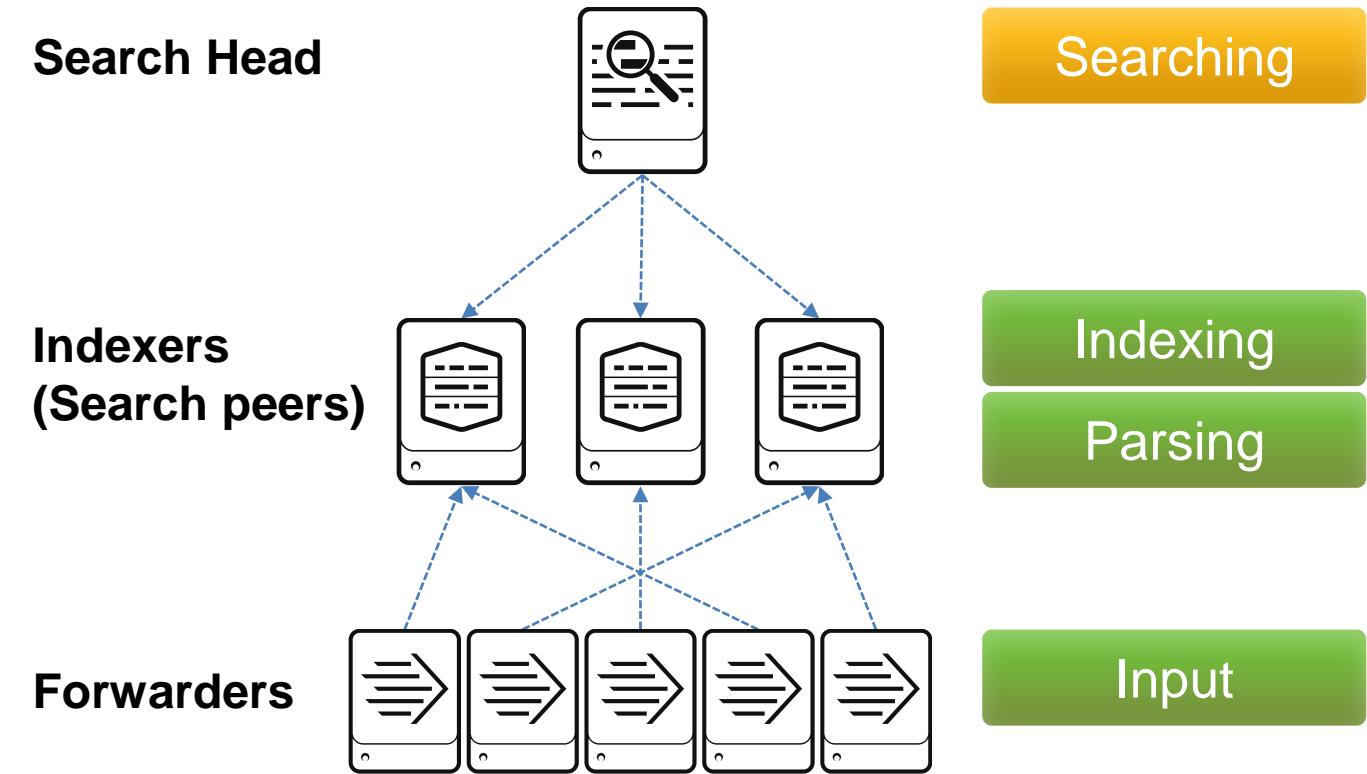


Basic Deployment for organizations:

- 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

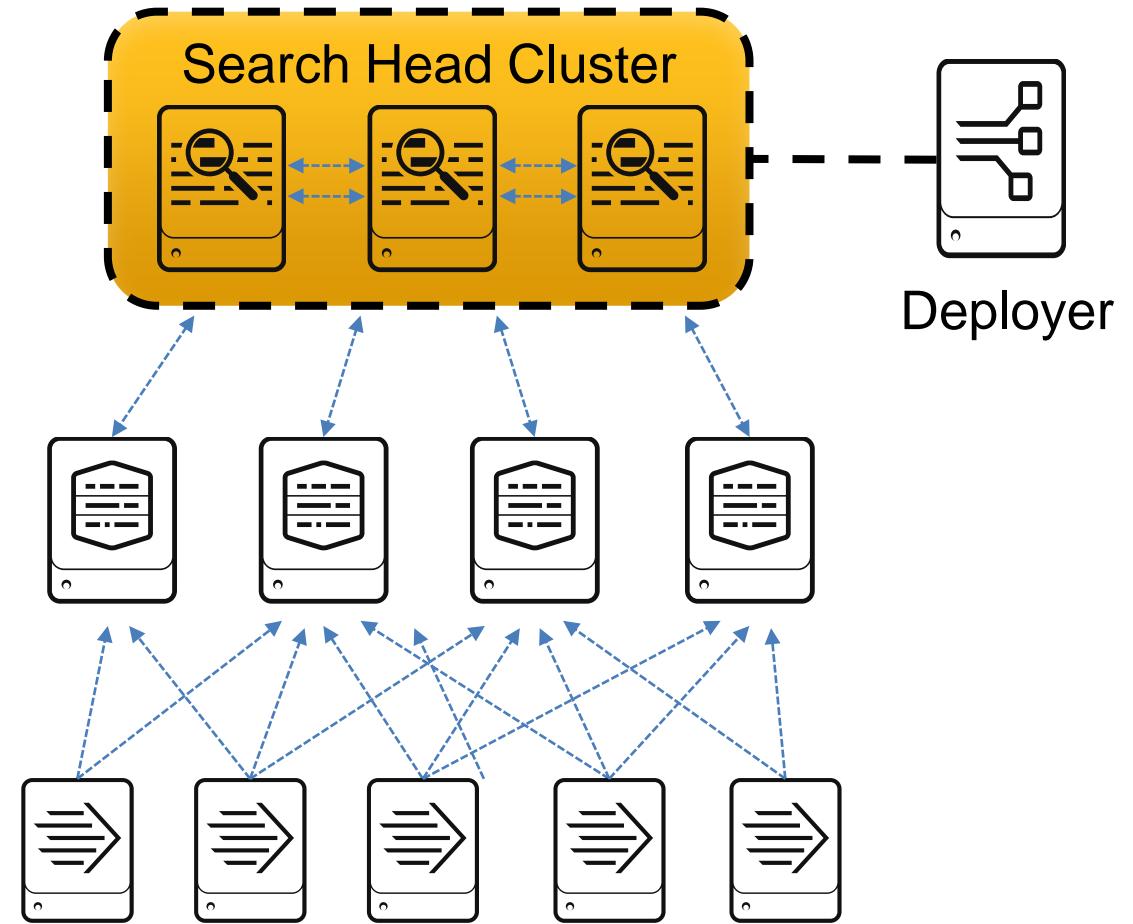


Deployment for organizations:

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

# Splunk Deployment – Increasing Capacity

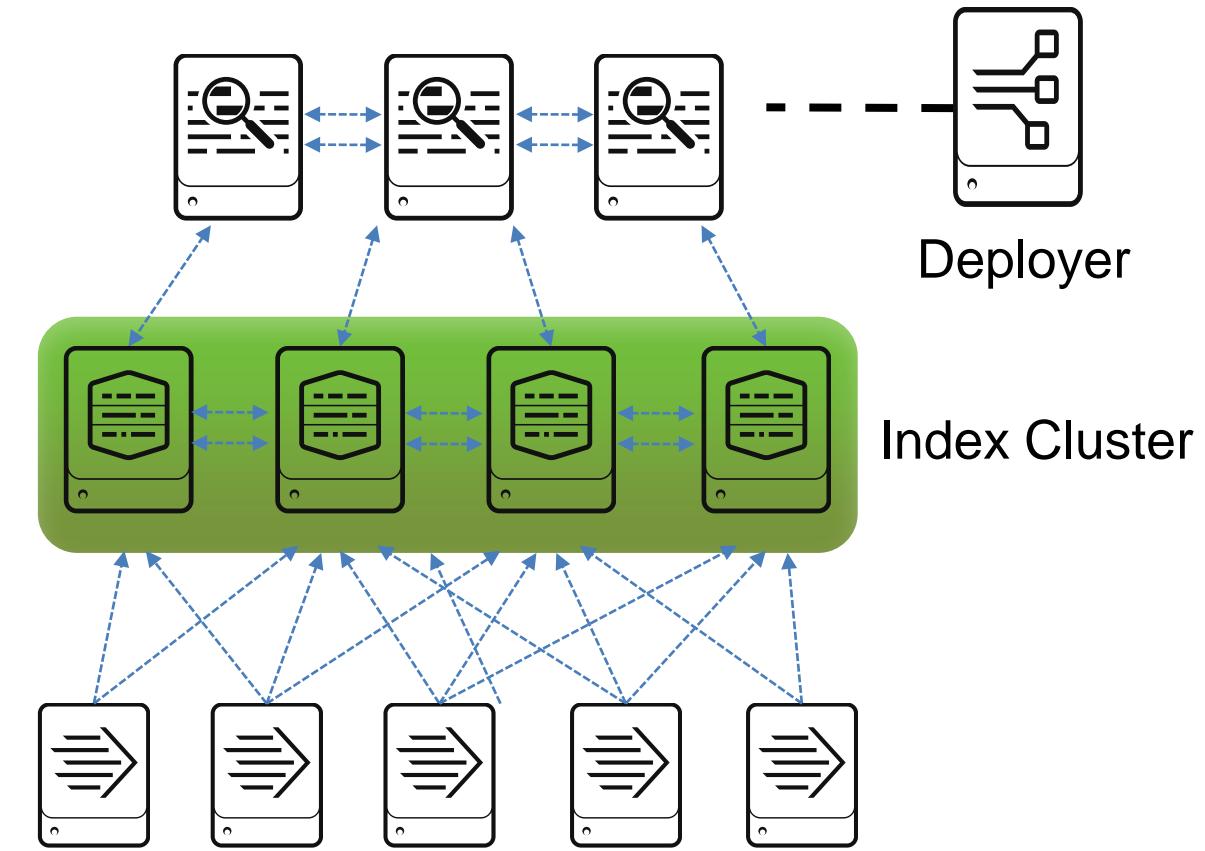
- Adding a Search Head Cluster:
  - Services more users for increased search capacity
  - Allows users and searches to share resources
  - Coordinate activities to handle search requests and distribute the requests across the set of indexers
- Search Head Clusters require a minimum of three Search Heads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



Generated for () (C) Splunk Inc, not for distribution

# 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



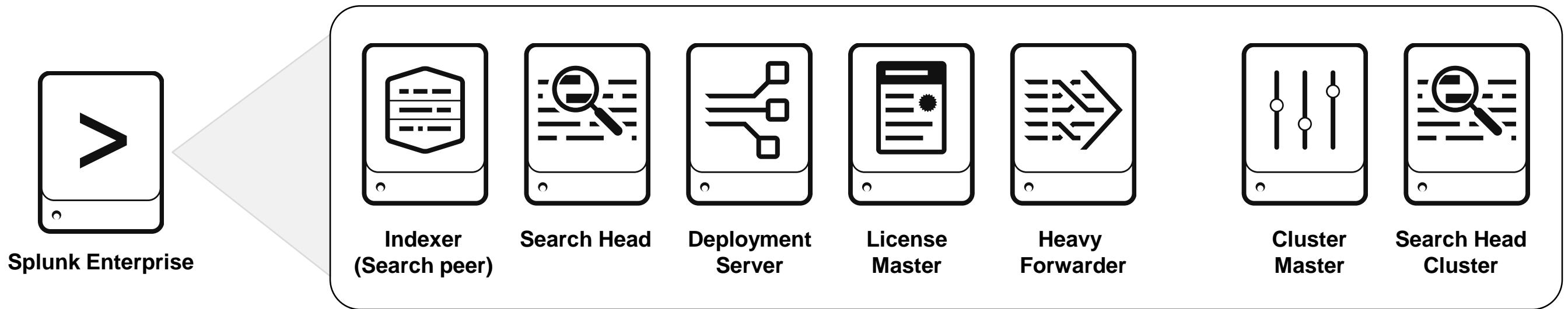
Generated for () (C) Splunk Inc, not for distribution

# Module 3: Installing Splunk

Generated for () (C) Splunk Inc, not for distribution

# Splunk Enterprise Install Package

There are multiple Splunk components installed from the Splunk Enterprise package



Generated for () (C) Splunk Inc, not for distribution

# Splunk Enterprise Installation Overview

---

- Verify required ports are open (splunkweb, splunkd, forwarder) and start-up account
- Download Splunk Enterprise from [www.splunk.com/download](http://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](http://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

Generated for () (C) Splunk Inc, not for distribution

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

Generated for () (C) Splunk Inc, not for distribution

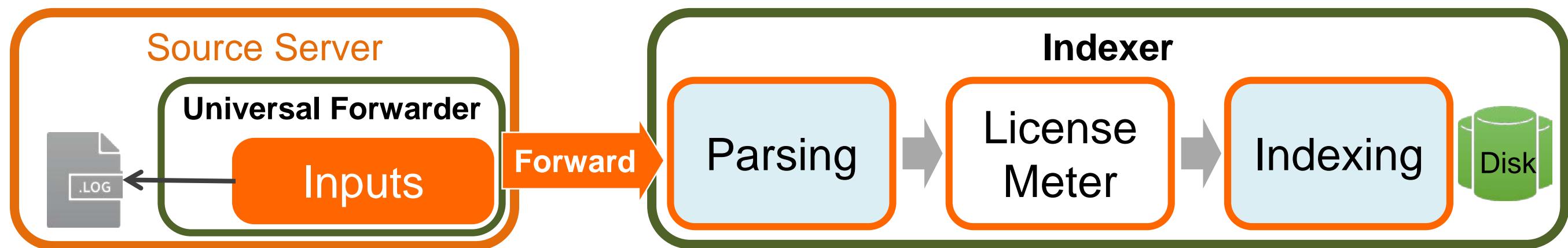
# Module 4

# Getting Data In

Generated for () (C) Splunk Inc, not for distribution

# Splunk Index Time Process

- Splunk index time process (data ingestion) can be broken down into three phases:
  1. **Input phase:** handled at the source (usually a forwarder)
    - The data sources are being opened and read
    - Data is handled as streams and any configuration settings are applied to the entire stream
  2. **Parsing phase:** handled by indexers (or heavy forwarders)
    - Data is broken up into events and advanced processing can be performed
  3. **Indexing phase:**
    - License meter runs as data and is initially written to disk, prior to compression
    - After data is written to disk, it **cannot** be changed



Generated for () (C) Splunk Inc, not for distribution

# Data Input Types

---

- Splunk supports many types of data input
  - **Files and directories:** monitoring text files and/or directory structures containing text files
  - **Network data:** listening on a port for network data
  - **Script output:** executing a script and using the output from the script as the input
  - **Windows logs:** monitoring Windows event logs, Active Directory, etc.
  - **HTTP:** using the HTTP Event Collector
  - And more...
- You can add data inputs with:
  - Apps and add-ons from Splunkbase
  - Splunk Web
  - CLI
  - Directly editing **inputs.conf**

Generated for () (C) Splunk Inc, not for distribution

# Default Metadata Settings

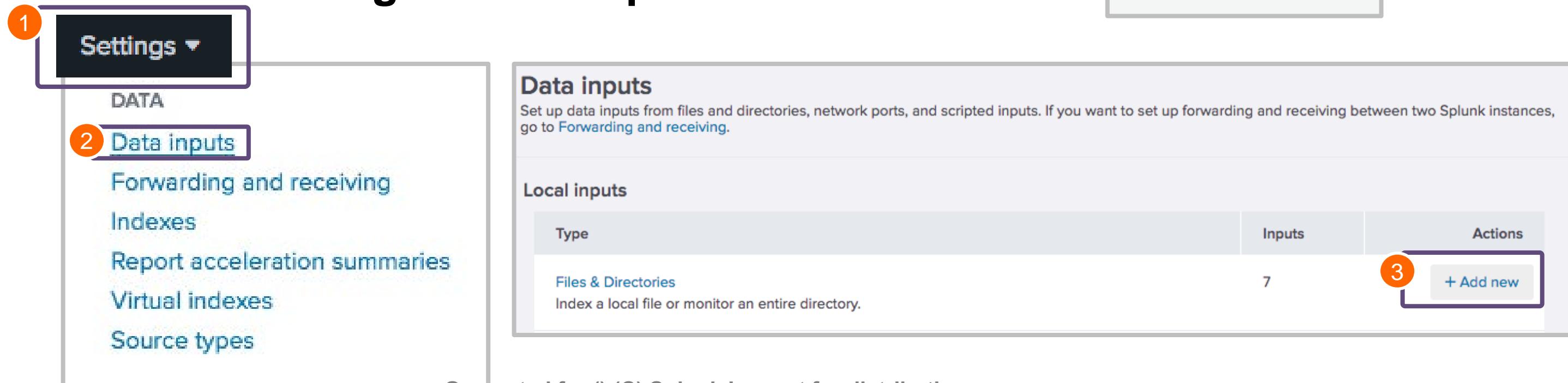
- When you index a data source, Splunk assigns metadata values
  - The metadata is applied to the entire source
  - Splunk applies defaults if not specified
  - You can also override them at input time or later

| Metadata          | Default   |
|-------------------|---|
| <b>source</b>     | Path of input file, network hostname:port, or script name         |
| <b>host</b>       | Splunk hostname of the inputting instance (usually a forwarder)   |
| <b>sourcetype</b> | Uses the source filename if Splunk cannot automatically determine |
| <b>index</b>      | Defaults to <b>main</b>   |

Generated for () (C) Splunk Inc, not for distribution

# Adding an Input with Splunk Web

- Splunk admins have a number of ways to start the **Add Data** page
  - Click the **Add Data** icon
    - › On the admin's **Home** page
    - › On the **Settings** panel
  - Select **Settings > Data inputs > Add new**



The screenshot shows the Splunk Web interface for adding data inputs. The left sidebar has a purple outline around the 'Settings' dropdown, with the number '1' in an orange circle above it. The 'Data inputs' link in the sidebar is highlighted with a purple outline and the number '2' in an orange circle above it. The main content area shows the 'Data inputs' page with a sub-section for 'Local inputs'. A table lists 'Files & Directories' with 7 entries. The 'Actions' column for the last entry shows a button labeled '+ Add new' with the number '3' in an orange circle above it.

Generated for () (C) Splunk Inc, not for distribution

# Add Data Menu

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

**Add Data**

How do you want to add data?

 **Upload**  
files from my computer

 **Monitor**  
files and ports on this Splunk indexer

 **Forward**  
data from Splunk forwarder

**Upload Option**

Upload allows uploading local files that only get indexed once. Useful for testing or data that is created once and never gets updated. Does not create **inputs.conf**.

**Monitor Option**

Provides one-time or continuous monitoring of files, directories, http events, network ports, or data gathering scripts located on Splunk Enterprise instances. Useful for testing inputs.

**Forward Option**

Main source of input in production environments. Remote machines gather and forward data to indexers over a receiving port.

Generated for () (C) Splunk Inc, not for distribution

# Select Source

1 Select the **Files & Directories** option to configure a monitor input

2 To specify the source:

- Enter the absolute path to a file or directory, or
- Use the **Browse** button

3 For ongoing monitoring  
For one-time indexing (or testing); the **Index Once** option does not create a stanza in `inputs.conf`

Add Data

Select Source Type

Input Settings

Review

Done

Back

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 any API, service, or database with a script.

File or Directory ?  Browse

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

Continuously Monitor

Index Once

Whitelisted?

Blacklist ?

Generated for () (C) Splunk Inc, not for distribution

# Set Source Type (Data Preview Interface)

## 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: /opt/log/www1/access.log View Event Summary

1 Source type: access\_combined\_wcookie ▾ Save As

2 filter 3

4

|   | Time                       | Event  |
|---|----------------------------|--|
| 1 | 11/28/17<br>4:58:01.000 PM | 111.161.27.20 - - [Nov/2017:16:58:01] "GET /cart.do?action=remove&itemId=EST-19&productId=PZ-SG-G05&JSESSIONID=SD6SL1FF4ADFF4960 HTTP 1.1" 200 2708 "http://www.buttercupgames.com" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 72  |
| 2 | 11/28/17<br>4:58:03.000 PM | 111.161.27.20 - - [28/Nov/2017:16:58:03] "GET /cart.do?action=changequantity&itemId=EST-19&productId=MB-AG-T01&JSESSIONID=SD6SL1FF4ADFF4960 HTTP 1.1" 200 2016 "http://www.buttercupgames.com/product.screen?productId=MB-AG-T01" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 418 |
| 3 | 11/28/17<br>4:58:09.000 PM | 111.161.27.20 - - [28/Nov/2017:16:58:09] "GET /category.screen?categoryId=NULL&JSESSIONID=SD6SL1FF4ADFF4960 HTTP 1.1" 406 552 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-21" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 283                                   |
| 4 | 11/28/17<br>00 PM          | 111.161.27.20 - - [28/Nov/2017:16:58:14] "GET /search.do?items=2112&JSESSIONID=SD6SL1FF4ADFF4960 HTTP 1.1" 404 3162 "http://www.buttercupgames.com/oldlink?itemId=EST-19" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 126   |
|   |                            | 111.161.27.20 - - [28/Nov/2017:16:58:19] "GET /cart.do?action=view&itemId=EST-27&productId=WC-SH-A01&JSESSIONID=SD6SL1FF4ADFF4960 HTTP 1.1" 200 1195 "http://www.buttercupgames.com/product.screen?productId=WC-SH-A01" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 273           |

Generated for () (C) Splunk Inc, not for distribution

# Set Source Type (cont.)

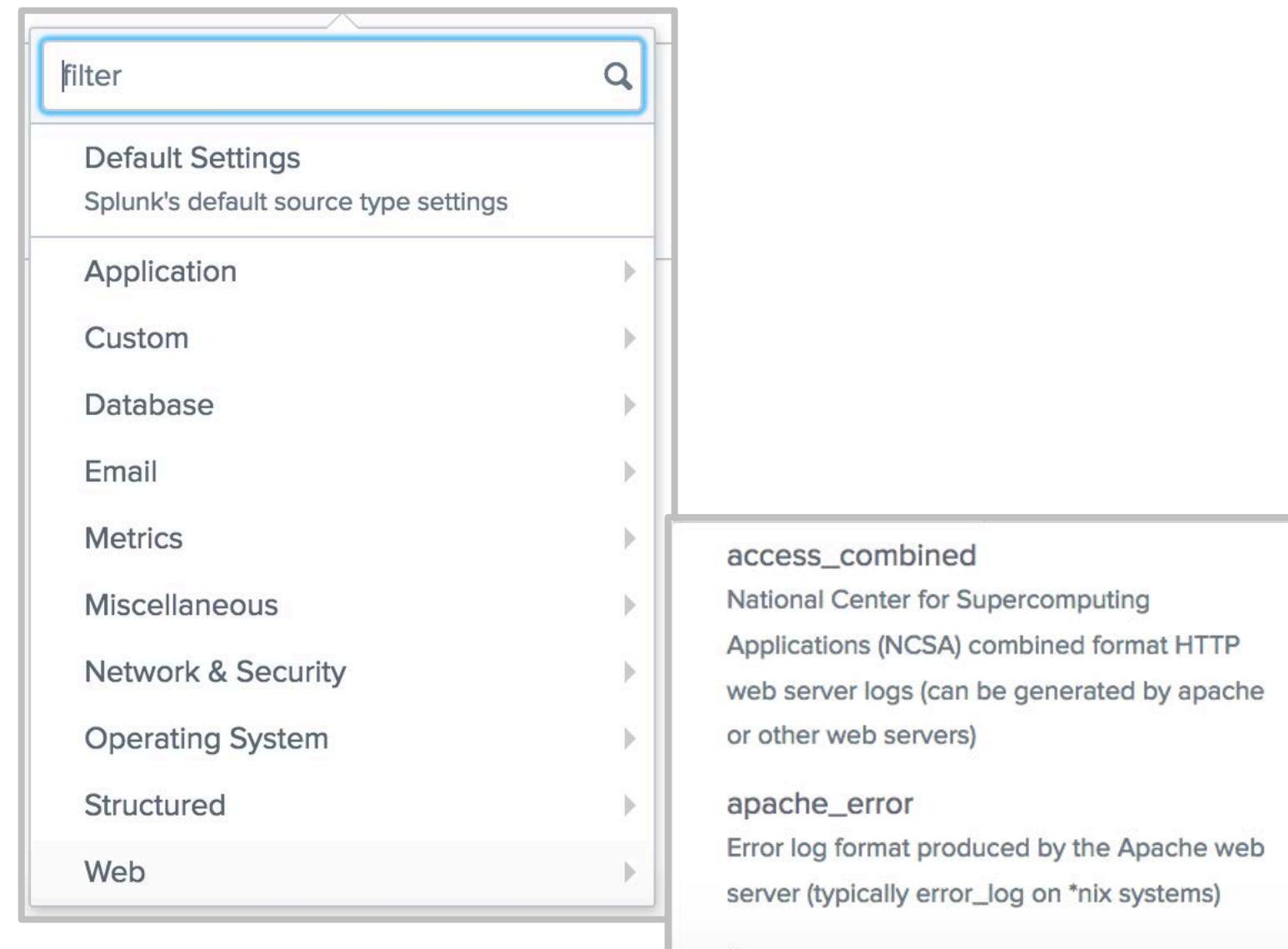
---

- ① Splunk automatically determines the source type for major data types when there is enough data
- ② You can choose a different source type from the dropdown list
- ③ Or, you can create a new source type name for the specific source
- ④ **Data preview** displays how your processed events will be indexed
  - If the events are correctly separated and the right timestamps are highlighted, you can move ahead
    - ▶ If not, you can select a different source type from the list or customize the settings

Generated for () (C) Splunk Inc, not for distribution

# Pretrained Source Types

- Splunk has default settings for many types of data
- The docs also contain a list of source types that Splunk automatically recognizes
- Splunk apps can be used to define additional source types



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

# Input Settings

The app context determines where your input configuration is saved

- The app context determines where your input configuration is saved
- In this example, it will be saved in:  
**SPLUNK\_HOME/etc/apps/search/local**

By default, the default host name in **General settings** is used

- Select the index where this input should be stored
- To store in a new index, first create the new index

Add Data

Select Source Set Source Type Input Settings Review Done

**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 you choose determines the available configuration 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](#)

App Context: Search & Reporting (search)

Host field value: splunk01

Index: itops

Create a new index

Generated for () (C) Splunk Inc, not for distribution

# Review

- Review the input configuration summary and click **Submit** to finalize

Add Data

Review

Input Type ..... File Monitor  
Source Path ..... /opt/log/www1/access.log  
Continuously Monitor ..... Yes  
Source Type ..... access\_combined\_wcookie  
App Context ..... search  
Host ..... splunk01  
Index ..... itops

Generated for () (C) Splunk Inc, not for distribution

# What Happens Next?

- Indexed events are available for immediate search
  - However, it may take a minute for Splunk to *start* indexing the data
- You are given other options to do more with your data

Add Data

Select Source   Set Source Type   Input Settings   Review   Done

< Back   Submit >

**Review**

|                            |                          |
|----------------------------|--------------------------|
| Input Type .....           | File Monitor             |
| Source Path .....          | /opt/log/www1/access.log |
| Continuously Monitor ..... | Yes                      |
| Source Type .....          | access_combined_wcookie  |
| App Context .....          | search                   |
| Host .....                 | splunk01                 |
| Index .....                | test                     |

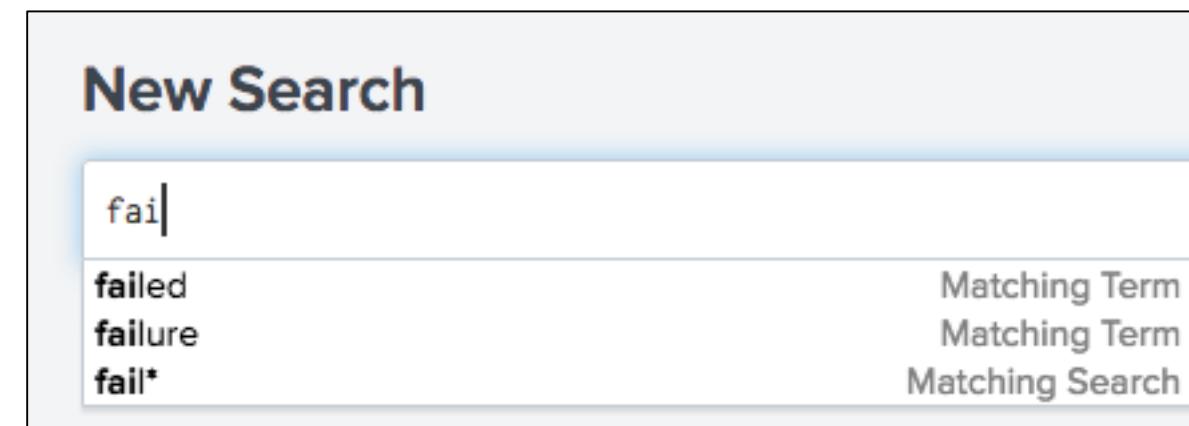
Generated for () (C) Splunk Inc, not for distribution

# Module 5: Basic Search

Generated for () (C) Splunk Inc, not for distribution

# Search Assistant

- Search Assistant provides selections for how to complete the search string
- Before the first pipe (|), it looks 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 () (C) Splunk Inc, not for distribution

# Search Assistant (cont.)

- After the first pipe, the Search Assistant shows 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 'New Search' interface. The search bar contains the query 'failed | cha'. Below the search bar, a dropdown menu lists several chart-related commands: 'chart', 'sichart', 'timechart', and 'sitimechart'. A tooltip for 'chart' provides a brief description: 'Returns results in a tabular output for charting.' and an example: '... | chart max(delay) over foo'. The 'Events (1,942)' section is visible at the bottom.

A screenshot of the Splunk 'New Search' interface showing the search bar with 'failed | chart cou'. The dropdown menu now includes additional chart-related commands: 'count', 'chart count by host', 'chart count by src\_ip', 'chart count by user', 'chart count(\_raw) by action', and 'chart count(\_raw) by saved\_search'. The 'Events (1,942)' section is still present at the bottom.

Generated for () (C) Splunk Inc, not for distribution

# Search Assistant (cont.)

- Search Assistant is enabled by default in the **SPL Editor** user preferences
- By default, **Compact** is selected
- To show more information, choose **Full**

**Compact Mode**

**New Search**

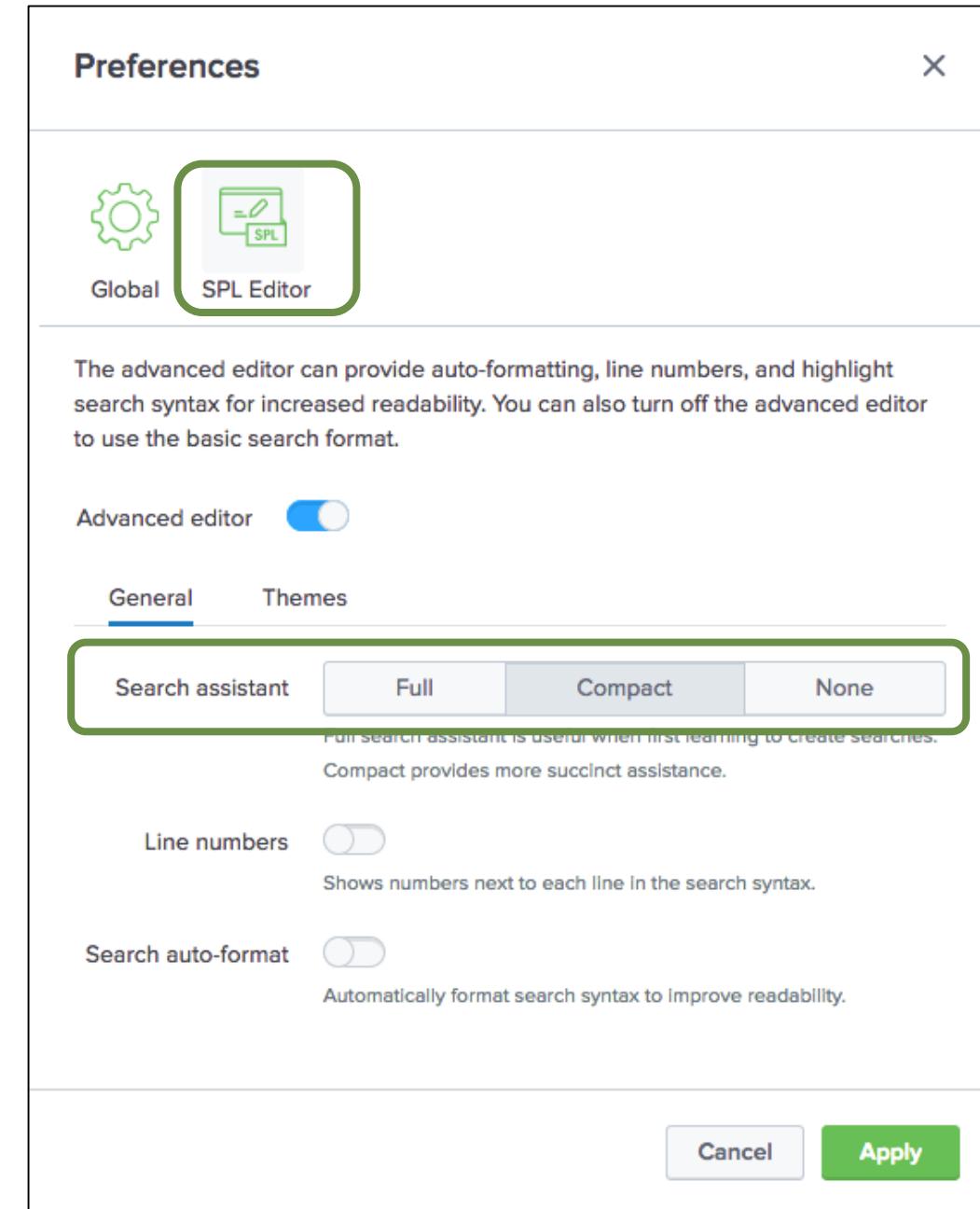
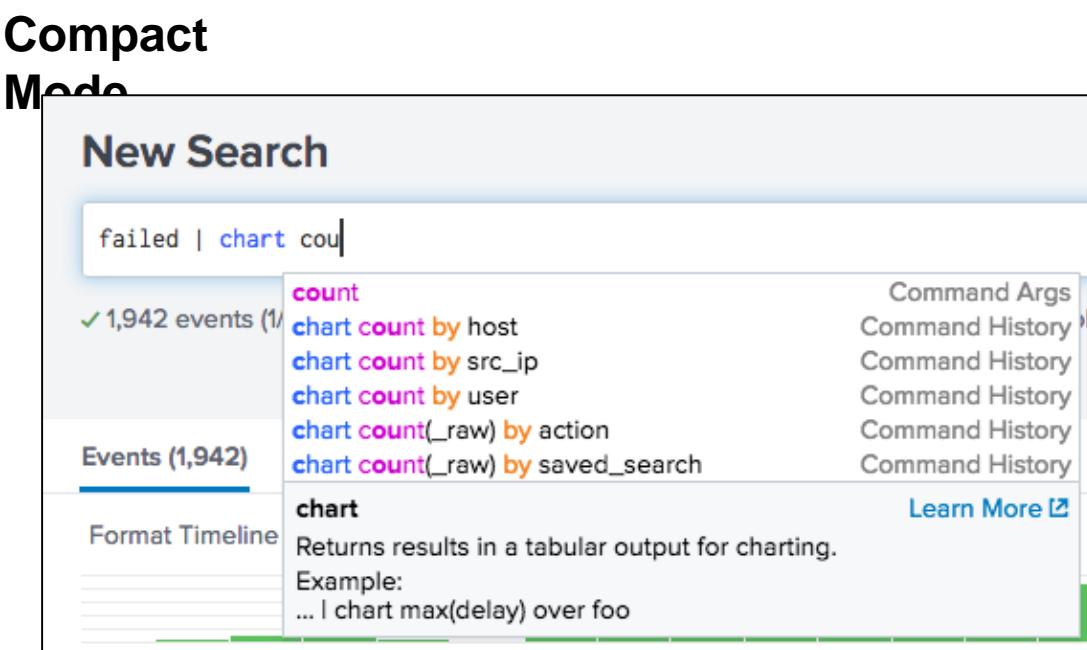
```
failed | chart cou
```

✓ 1,942 events (1/1)

Events (1,942)

Format Timeline

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



Generated for () (C) Splunk Inc, not for distribution

# Search Assistant – Full Mode

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

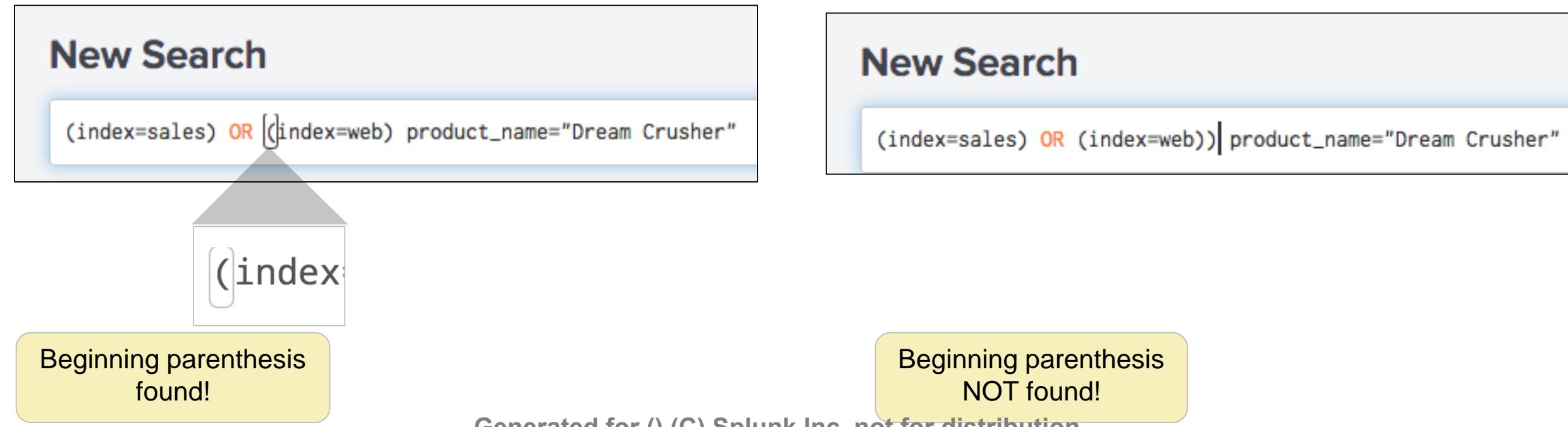
The screenshot shows the Splunk Search Assistant interface. A search bar at the top contains the query "failed | chart cou". Below the search bar, there's a "Command History" section with several previous search queries. On the right side, a detailed card for the "chart" command is displayed. The card includes a "Help" link, a "More »" button (circled in orange), and a note stating "Returns results in a tabular output for charting." It also lists "Examples" and "Command Args". A checkbox labeled "Auto Open" is checked. The entire card is circled in orange.

This screenshot shows the same interface but with the "Auto Open" checkbox unchecked, resulting in a simplified view. The "More »" button is now highlighted in blue (circled in orange), and the "Less" button is visible. The card for the "chart" command now includes a "Details" section describing how it creates a table of statistics suitable for charting. The rest of the interface remains similar to the first screenshot.

Generated for () (C) Splunk Inc, not for distribution

# Search Assistant – Parentheses

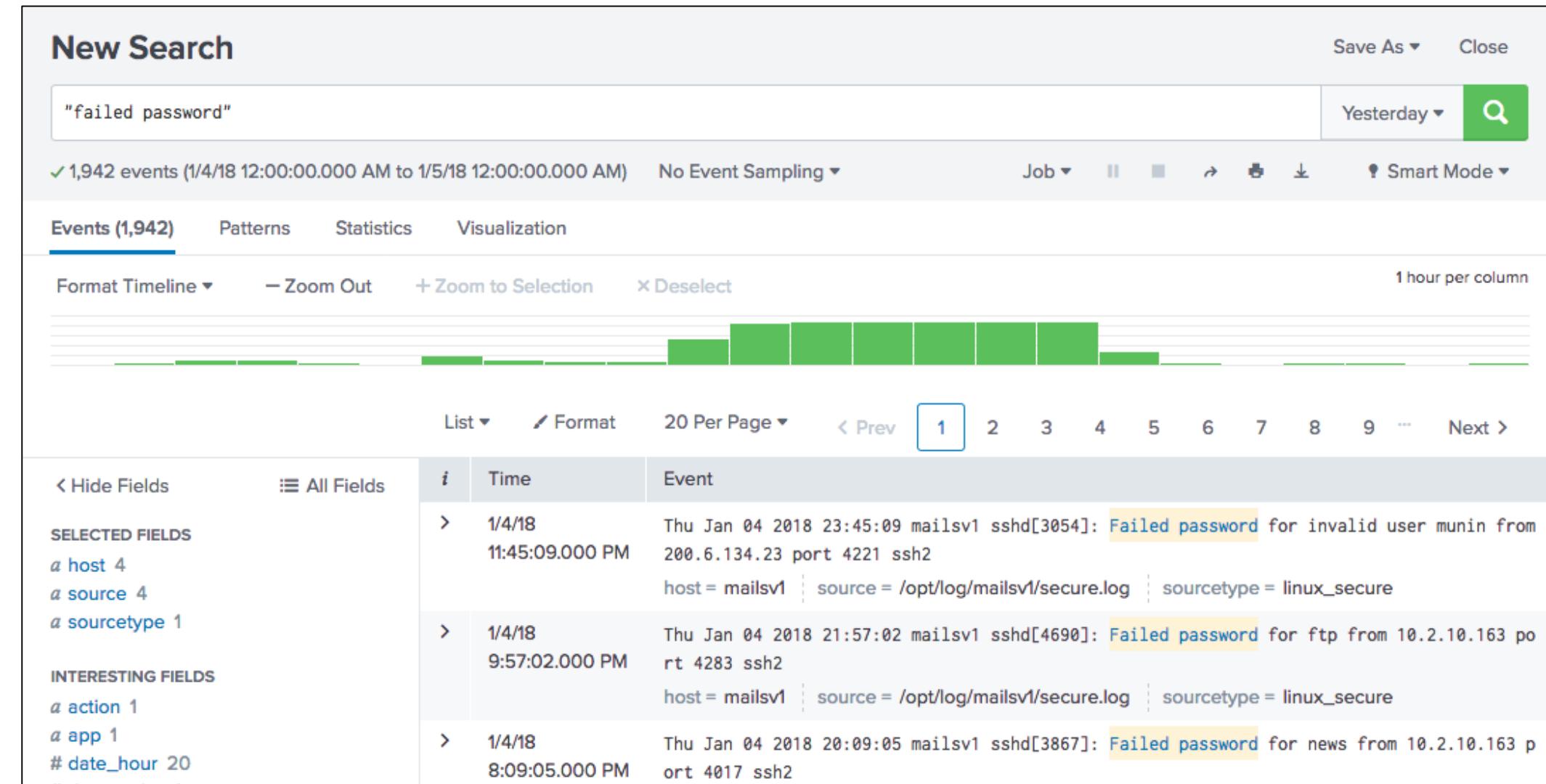
- The Search Assistant provides help to match parentheses as you type
- When an end parenthesis is typed, the corresponding beginning parenthesis is automatically highlighted
  - If a beginning parenthesis cannot be found, *nothing* is highlighted



Generated for () (C) Splunk Inc, not for distribution

# Viewing Search Results

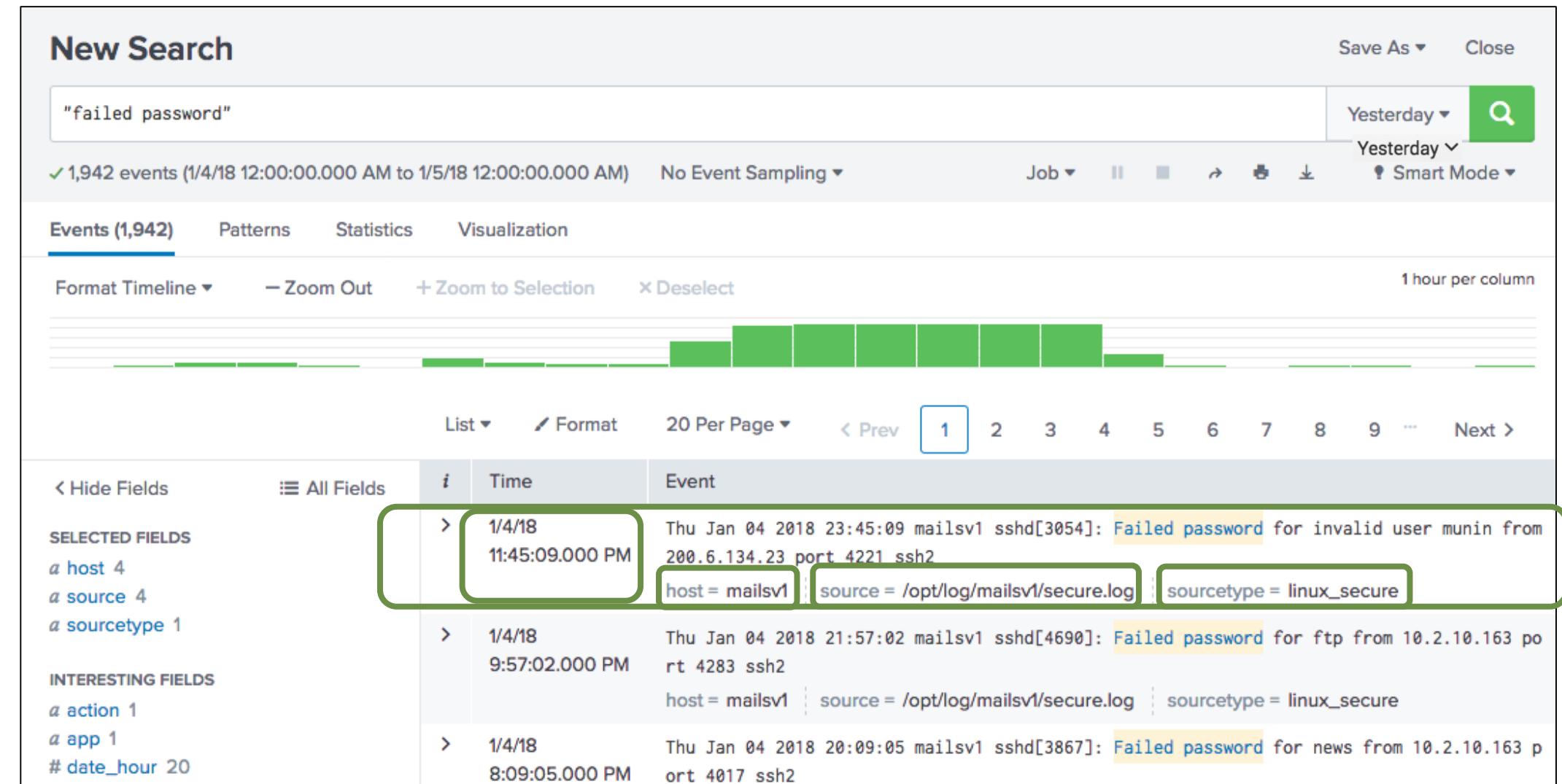
- Matching results are returned immediately
- Displayed in reverse chronological order (newest first)
- Matching search terms are highlighted



Generated for () (C) Splunk Inc, not for distribution

# Viewing Search Results (cont.)

- Splunk parses data into individual events, extracts time, and assigns metadata
- Each event has:
  - timestamp
  - host
  - source
  - sourcetype
  - index



Generated for () (C) Splunk Inc, not for distribution

# Viewing Search Results (cont.)

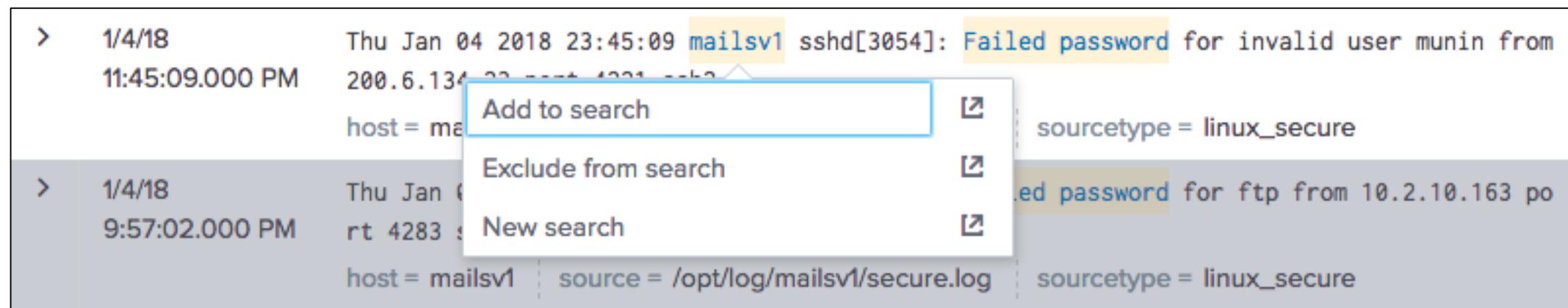
The screenshot shows the Splunk search interface with the following annotations:

- New Search**: The search bar contains the query `"failed password"`.
- time range picker**: Shows the search range from `1/4/18 12:00:00.000 AM` to `1/5/18 12:00:00.000 AM`, with a dropdown for `Yesterday` and a search icon.
- Events (1,942)**: The number of events found, with a green arrow pointing to it from the top-left.
- search mode**: A dropdown menu currently set to `Smart Mode`.
- timeline**: A timeline visualization showing event distribution over time.
- paginator**: A page navigation bar showing page 1 of 10, with a green border around the page number.
- Fields sidebar**: A sidebar listing selected fields (`host`, `source`, `sourcetype`) and interesting fields (`action`, `app`, `#date_hour`).
- timestamp**: A timestamp field in the results table, highlighted with a green box.
- selected fields**: A tooltip for the timestamp field showing the event details: `Thu Jan 04 2018 23:45:09 mailsv1 sshd[3054]: Failed password for invalid user munin from 200.6.134.23 port 4221 ssh2 host = mailsv1 source = /opt/log/mailsv1/secure.log sourcetype = linux_secure`.
- events**: A large green bracket on the right side grouping the results table and the event details.

Generated for () (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 () (C) Splunk Inc, not for distribution

# Changing Search Results View Options

You have several layout options for displaying your search results

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

- Search Bar:** "failed password" (1,942 events from 1/4/18 to 1/5/18).
- Time Range:** Yesterday.
- Events View (Top Right):** Shows raw log entries in a table format. The first entry is:

|                    |                             |         |                             |              |
|--------------------|-----------------------------|---------|-----------------------------|--------------|
| 11:45:09.000<br>PM | 1/4/18<br>9:57:02.000<br>PM | mailsv1 | /opt/log/mailsv1/secure.log | linux_secure |
|--------------------|-----------------------------|---------|-----------------------------|--------------|
- Event List View (Bottom Left):** Shows a list of events with their timestamp, host, source, and sourcetype.

| Time                   | Event   |
|------------------------|---|
| 1/4/18 11:45:09.000 PM | Thu Jan 04 2018 23:45:09 mailsv1 sshd[3054]: Failed password for invalid user munin from 200.6.134.23 port 4221 ssh2<br>host = mailsv1   source = /opt/log/mailsv1/secure.log   sourcetype = linux_secure |
| 1/4/18 9:57:02.000 PM  | Thu Jan 04 2018 21:57:02 mailsv1 sshd[4690]: Failed password for ftp from 10.2.10.163 port 4283 ssh2<br>host = mailsv1   source = /opt/log/mailsv1/secure.log   sourcetype = linux_secure                 |
| 1/4/18 8:09:05.000 PM  | Thu Jan 04 2018 20:09:05 mailsv1 sshd[3867]: Failed password for news from 10.2.10.163 port 4017 ssh2<br>host = mailsv1   source = /opt/log/mailsv1/secure.log   sourcetype = linux_secure                |
- Raw Log View (Bottom Right):** Shows raw log entries in a table format. The first entry is:

|   |
|---|
| 2018 23:45:09 mailsv1 sshd[3054]: Failed password for invalid user munin from 200.6.134.23 port |
|---|

Generated for () (C) Splunk Inc, not for distribution

# Selecting a Specific Time

The diagram illustrates the Splunk time range selection interface, divided into two main sections: 'Custom Time Ranges' (left) and 'Preset Time Ranges' (right).

**Custom Time Ranges:**

- Relative:** Set Earliest to 7 Days Ago and Latest to Now.
- Real-time:** Set Earliest to 7 Days Ago and Latest to now.
- Date Range:** Set Between 12/29/2017 and 01/05/2018, from 00:00:00 to 24:00:00.
- Date & Time Range:** Set Between 12/29/2017 at 11:00:00.000 and 01/05/2018 at 11:26:07.000.
- Advanced:** Set Earliest to -24h@h and Latest to now.

**Preset 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.
- OTHER:** Last 15 minutes, Last 60 minutes, Last 4 hours, Last 24 hours, Last 7 days, Last 30 days, All time.

A green bracket on the left groups the first five custom range sections, while a green bracket on the right groups the three preset sections. A yellow callout box labeled 'custom time ranges' points to the custom section bracket. A yellow callout box labeled 'preset time ranges' points to the preset section bracket.

Generated for () (C) Splunk Inc, not for distribution

# Time Range Abbreviations

- Time ranges are 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

earliest=6/15/2017:12:30:00

looks back to specified time

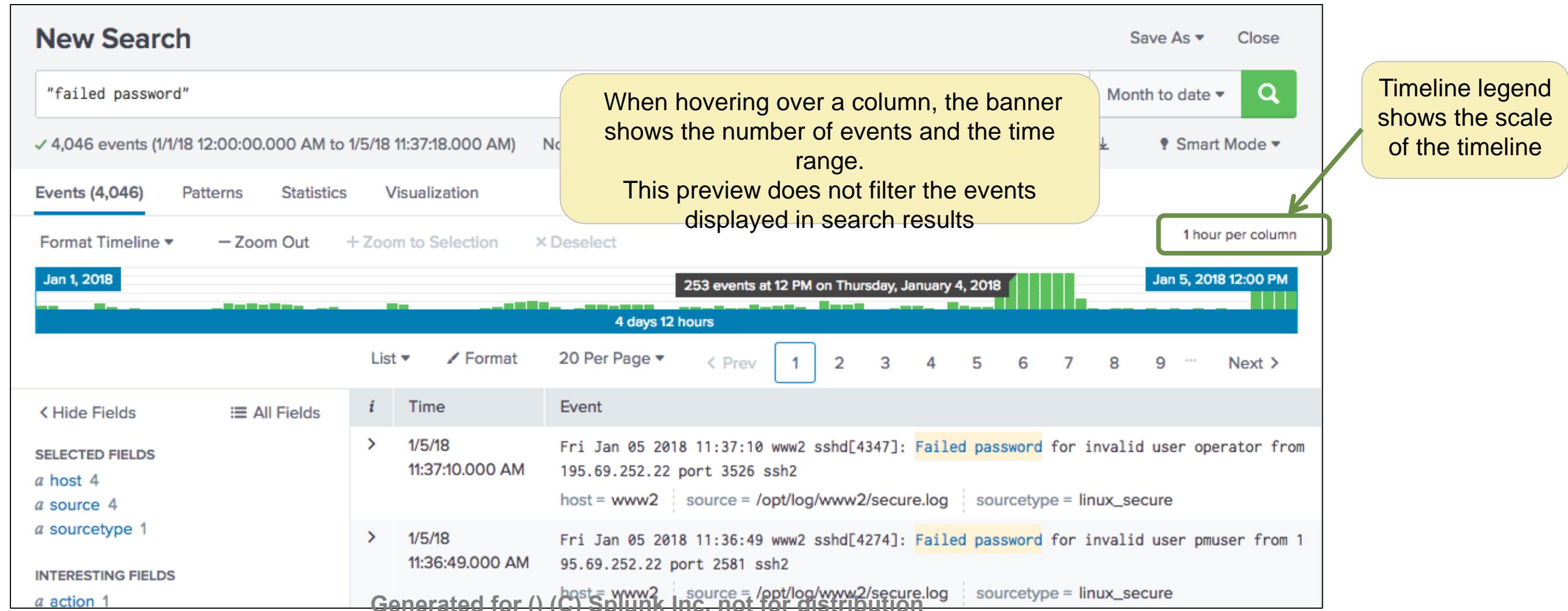
Note



If time specified, it must be in  
MM/DD/YYYY:HH:MM:SS format.

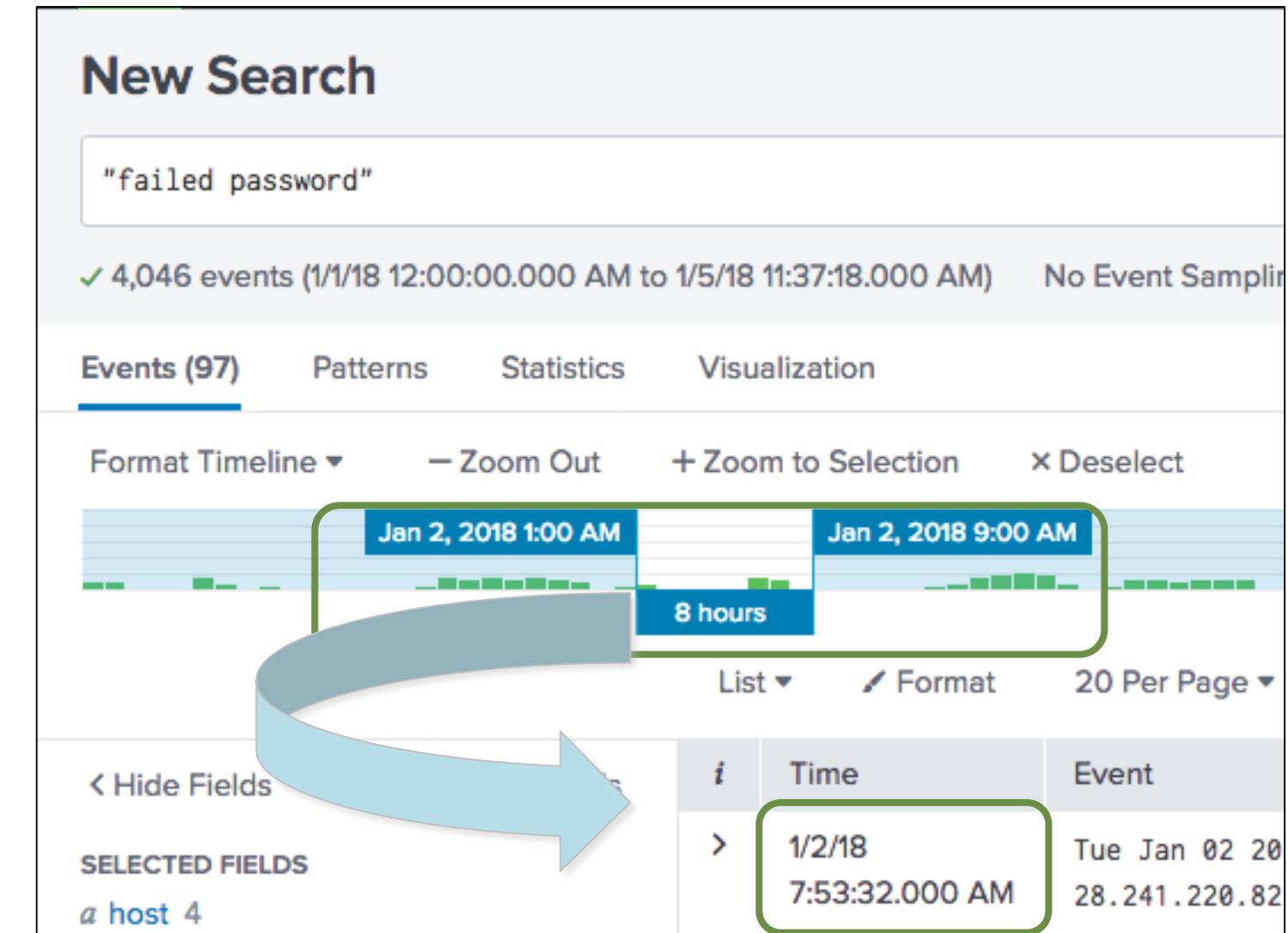
# Viewing the Timeline

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



# Viewing 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)



Generated for () (C) Splunk Inc, not for distribution

# Using Other Timeline Controls

- **Format Timeline**

- Hides or shows the timeline in different views

- **Zoom Out**

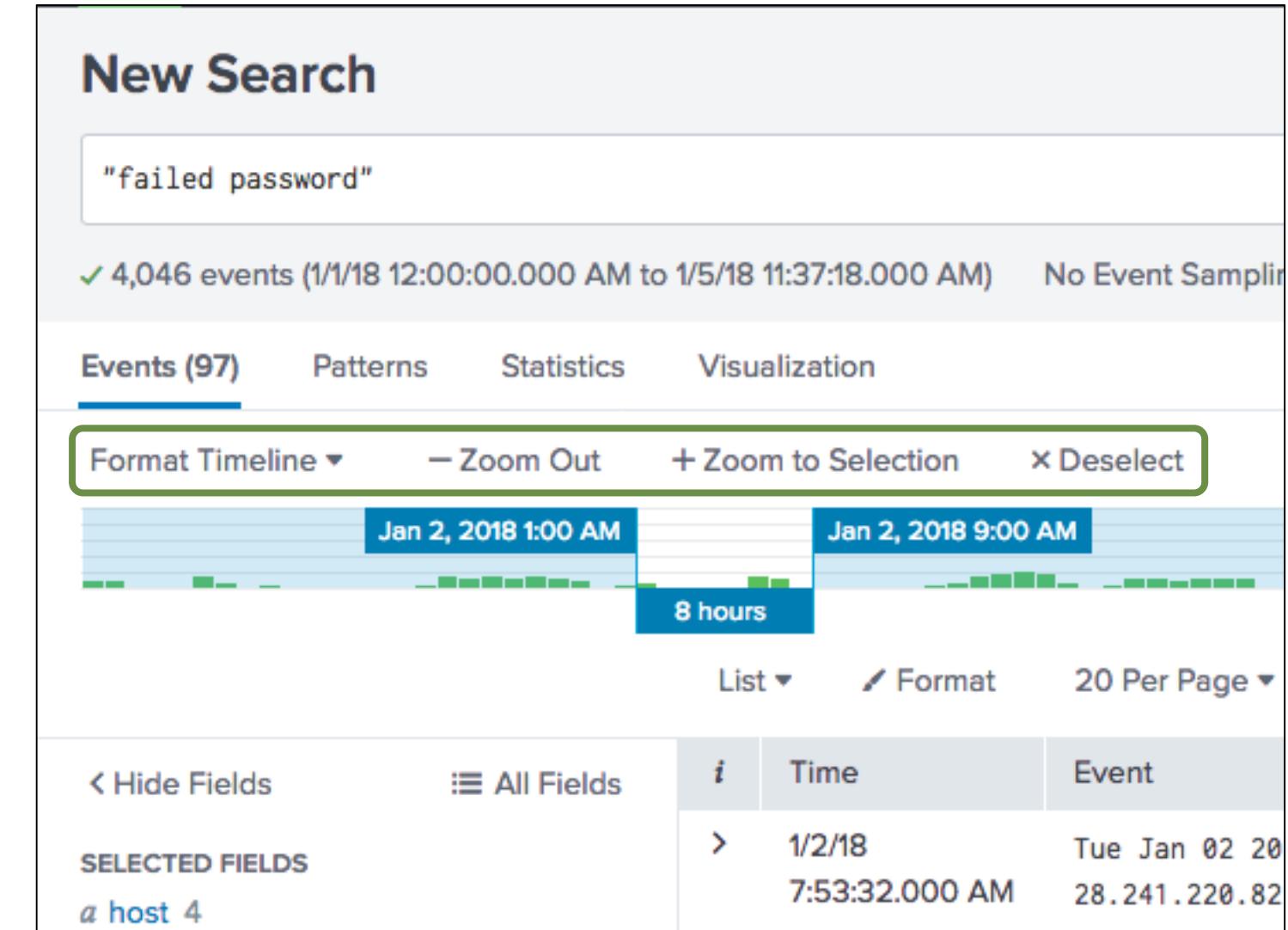
- Expands the time focus and re-executes the search

- **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 () (C) Splunk Inc, not for distribution

# Controlling and Saving Search Jobs

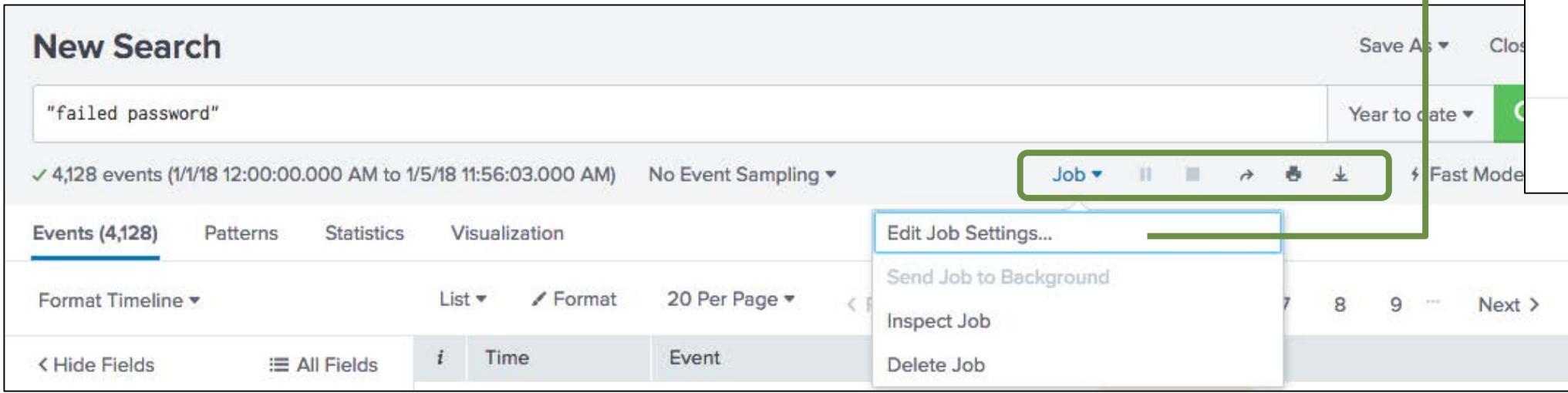
- Every search is also a **job**
- Use the Job bar to control search execution

 **Pause** – toggles to resume the search

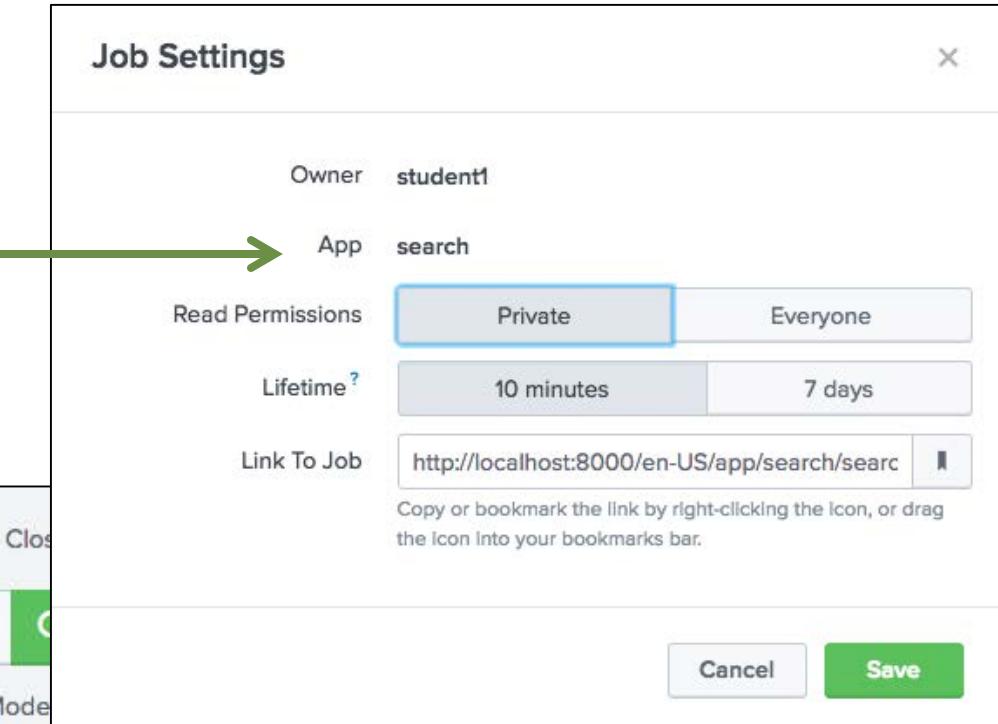
 **Stop** – finalizes the search in progress

– Jobs are available for 10 minutes (default)

– Get a link to results from the **Job** menu



The screenshot shows the Splunk interface with a search bar containing the query "failed password". Below the search bar, it displays "4,128 events (1/1/18 12:00:00.000 AM to 1/5/18 11:56:03.000 AM)" and "No Event Sampling". The "Events (4,128)" tab is selected. A context menu is open over the Job bar, with the "Edit Job Settings..." option highlighted. The Job bar itself includes icons for Pause, Stop, and other controls, along with a "Fast Mode" toggle.



# Setting Permissions

- **Private [default]**

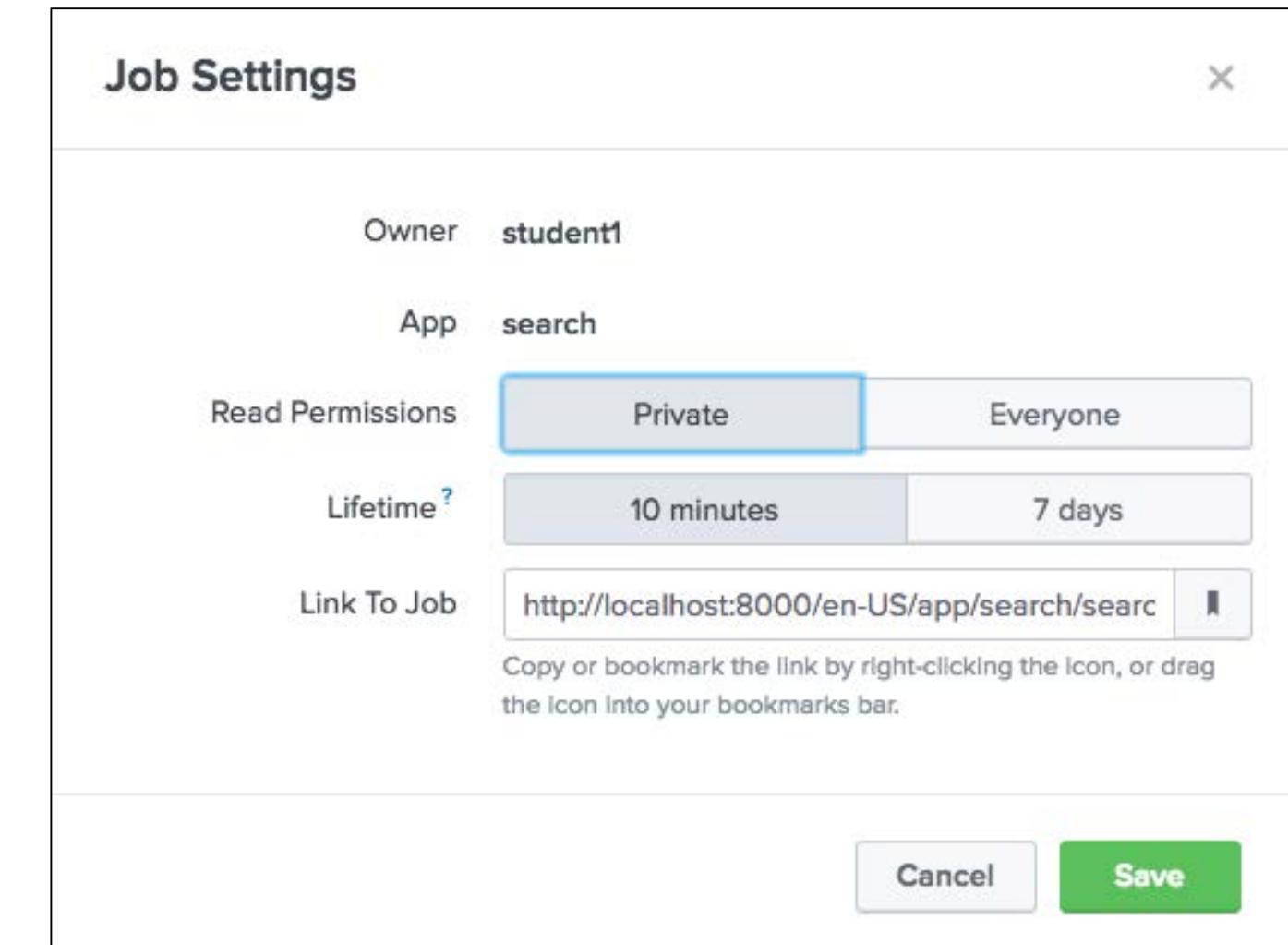
- Only the creator can access

- **Everyone**

- All app users can access search results

- **Lifetime**

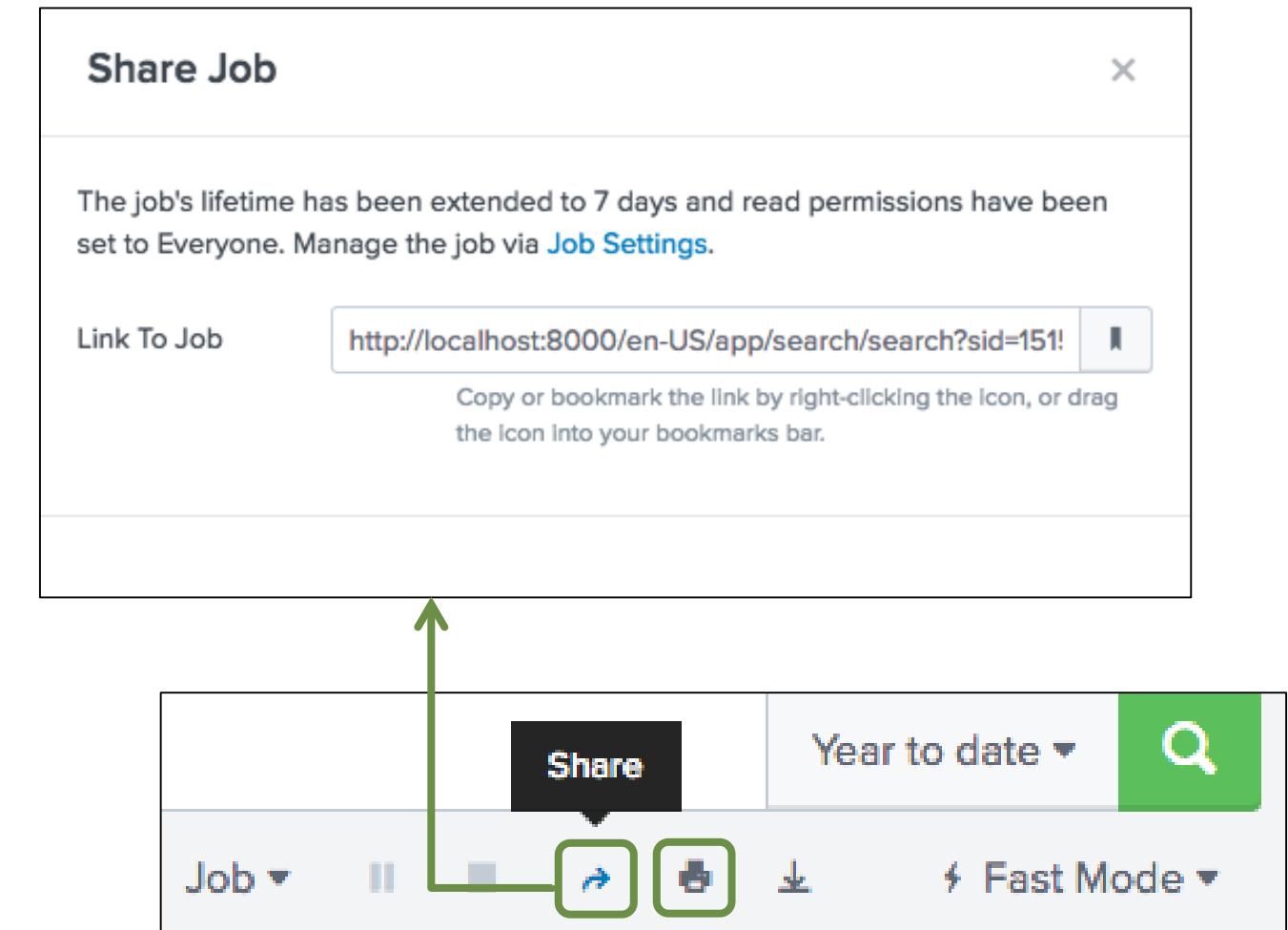
- Default is 10 minutes
  - Can be extended to 7 days
  - To keep your search results longer, schedule a report



Generated for () (C) Splunk Inc, not for distribution

# Sharing Search Jobs

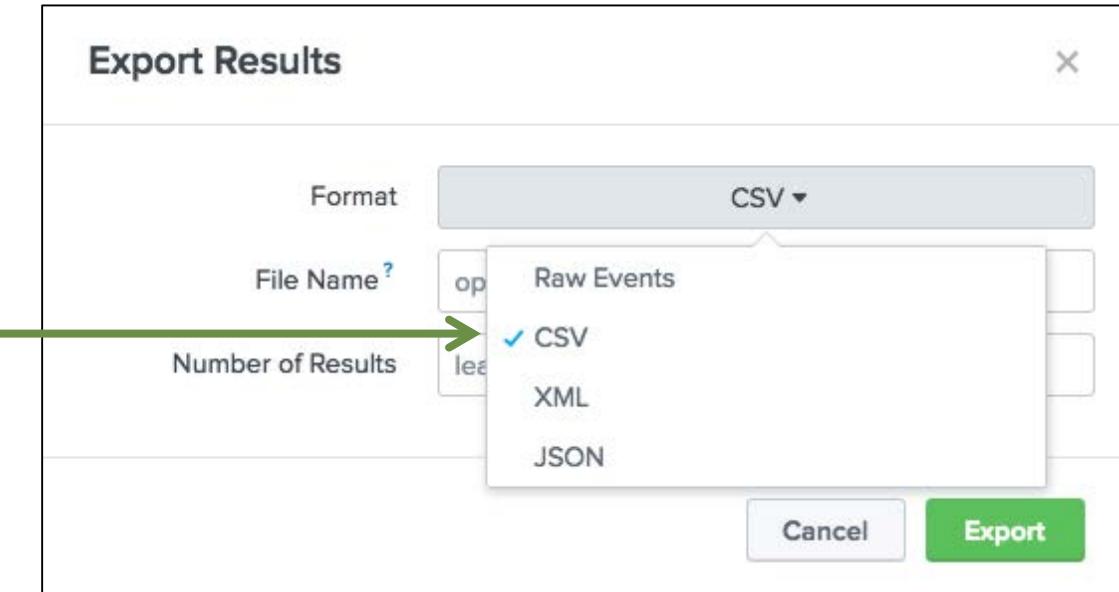
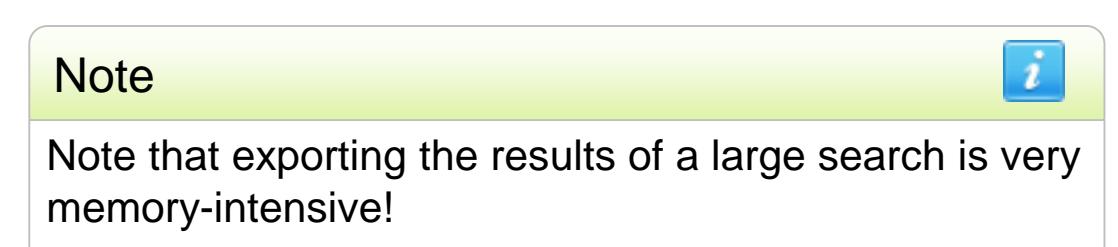
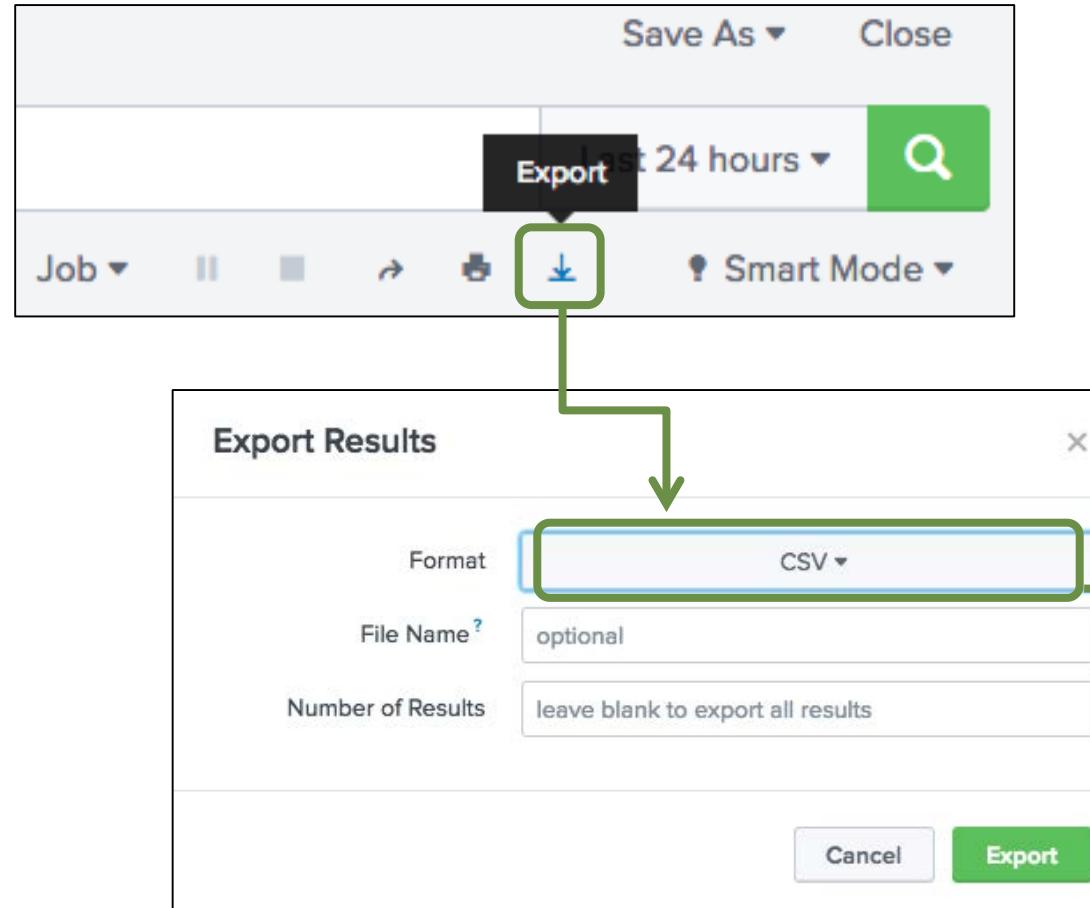
- Use the Share button next to the Job bar to quickly:
  - Give everyone read permissions
  - Extend results retention to 7 days
  - Get a sharable link to the results
- Sharing search allows multiple users working on same issue to see same data
  - More efficient than each running search separately
  - Less load on server and disk space used



- Can also click printer icon to print results or save as PDF

# Exporting Search Results

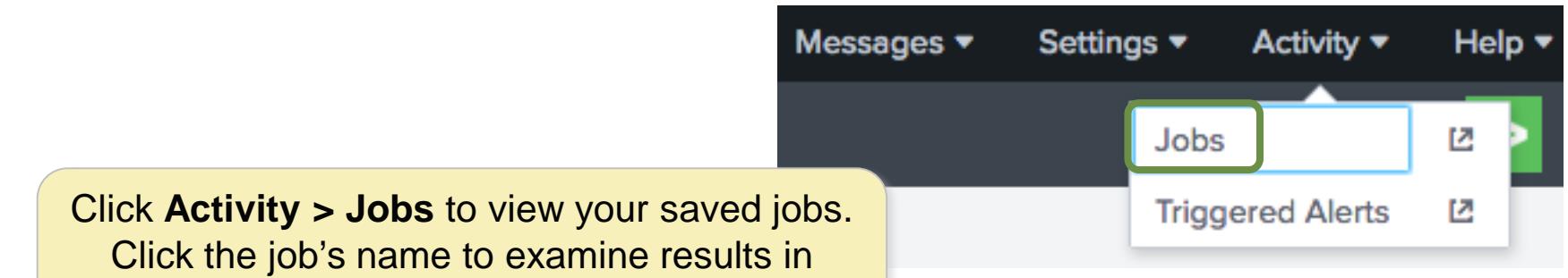
For an external copy of the results, **export** search results to Raw Events (text file), CSV, XML, or JSON format



Generated for () (C) Splunk Inc, not for distribution

# Viewing Your Saved Jobs

- 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.)

| 3 Jobs   |                                   | App: Search & Reporting (search) ▾ |               | Filter by owner ▾ |                         | Status: All ▾          | filter    | 10 Per Page ▾ |        |         |
|--|-----------------------------------|------------------------------------|---------------|-------------------|-------------------------|------------------------|-----------|---------------|--------|---------|
|  |                                   | Edit Selected ▾                    |               |                   |                         |                        |           |               |        |         |
|  |                                   | Owner ▾                            | Application ▾ | Events ▾          | Size ▾                  | Created at ▾           | Expires ▾ | Runtime ▾     | Status | Actions |
| >  | <input type="checkbox"/> student1 | search                             | 2,449         | 616 KB            | Jan 5, 2018 12:45:47 PM | Jan 5, 2018 1:02:50 PM | 00:00:01  | Done          | Job ▾  | ■ ↻ ↓   |
| <a href="#">"failed password"</a> [1/4/18 12:00:00.000 PM to 1/5/18 12:45:47.000 PM] |                                   |                                    |               |                   |                         |                        |           |               |        |         |

Generated for () (C) Splunk Inc, not for distribution

# Viewing 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

3. Click the > icon in the leftmost column to expand long queries to display the full text

The screenshot shows the Splunk search interface. At the top, there are tabs for Search, Datasets, Reports, Alerts, and Dashboards. On the right, there's a green button labeled 'Search & Reporting' with a right-pointing arrow. Below the tabs, there's a search bar with placeholder text 'enter search here...' and a dropdown for 'Last 24 hours'. To the right of the search bar is a magnifying glass icon. Further down, there's a 'Smart Mode' dropdown.

In the center, there's a 'Search' section with a 'How to Search' area containing links to 'Documentation' and 'Tutorial'. To the right, there's a 'What to Search' summary: '537,902 Events' (INDEXED), '3 months ago' (EARLIEST EVENT), and 'a few seconds ago' (LATEST EVENT).

A large callout box highlights the 'Search History' button (step 1). Below it, a dropdown menu titled 'Search History' is open, showing a list of time filters: 'No Time Filter' (selected), 'Ran: Today', 'Ran in: Last 7 Days', and 'Ran in: Last 30 Days'. Step 2 points to the 'No Time Filter' button. Step 3 points to the 'i' icon next to the first search result, which is expanded to show its full query: '(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'. Below this, three other search results are listed: "'failed password'", '(index=sales) OR (index=web) product\_name="Dream Crusher"', and 'index="failed password"'.

At the bottom of the search results table, there's a note: 'Generated for () (C) Splunk Inc, not for distribution'.

# Module 6: Using Fields in Searches

Generated for () (C) Splunk Inc, not for distribution

# 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, AND is implied unless otherwise specified

area\_code=404

action=purchase status=503

source=/var/log/messages\* NOT host=mail12

sourcetype=access\_combined

Generated for () (C) Splunk Inc, not for distribution

# Field Discovery

- Splunk automatically discovers many fields based on sourcetype and key/value pairs found in the data
- Prior to search time, some fields are already stored with the event in the index:
  - Meta fields, such as `host`, `source`, `sourcetype`, and `index`
  - Internal fields such as `_time` and `_raw`
- At search time, *field discovery* discovers fields directly related to the 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   |
|---|--------------------------|---|
| > | 1/5/18<br>1:21:10.000 PM | 192.162.19.179 - - [05/Jan/2018:13:21:10] "POST /cart/success.do?JSESSIONID=SD1SL6FF4ADFF4964 HT<br>TP 1.1" 200 966 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-26" "Mozilla/5<br>.0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version<br>/5.0.2 Mobile/8L1 Safari/6533.18.5" 552 |

## Note



For more information, please see:

<http://docs.splunk.com/Documentation/Splunk/latest/Data/Listofpretrainedsourcetypes>

Generated for () (C) Splunk Inc, not for distribution

# 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

New Search  
"failed password"  
✓ 2,406 events (1/4/18 1:00:00.000 PM to 1/5/18 1:36:10.000 PM) No Event Sampling ▾

Events (2,406) Patterns Statistics Visualization Format Timeline ▾ List ▾ Format 20 Per Page ▾

◀ Hide Fields ⌂ All Fields i Tim click to view all fields

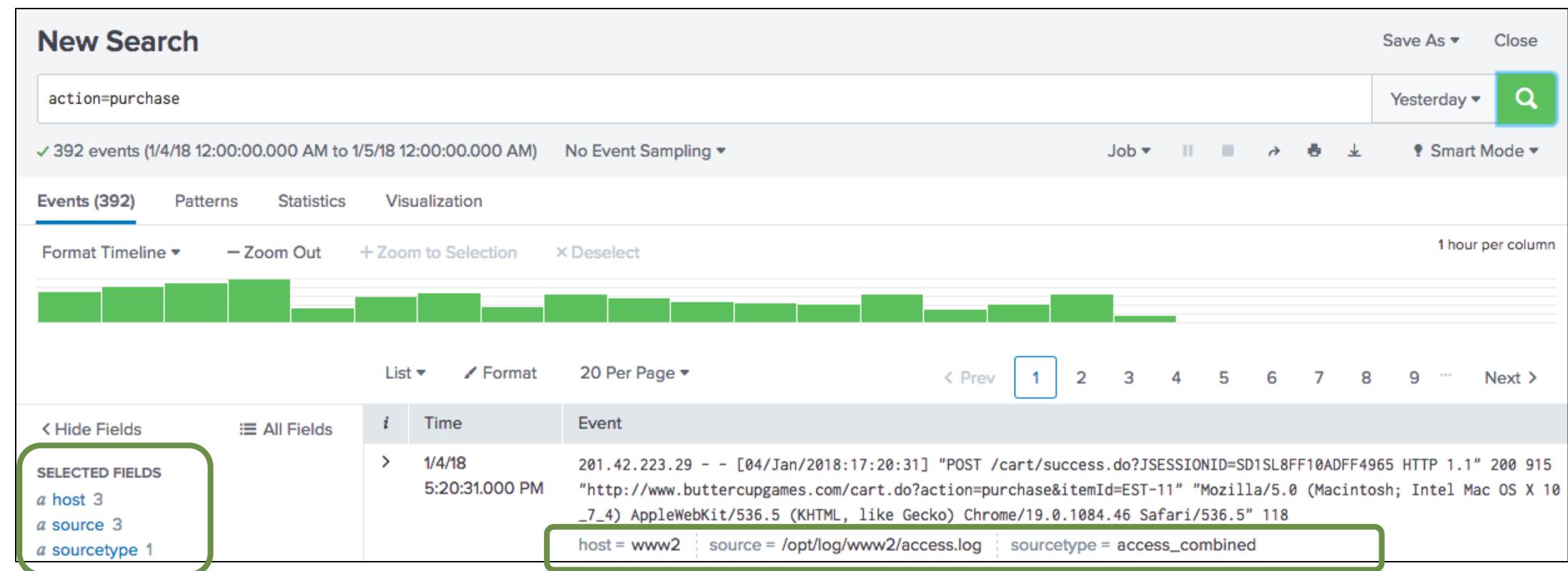
SELECTED FIELDS  
a host 4  
a source 4  
a sourcetype 1

INTERESTING FIELDS  
a action 1  
a app 1  
# date\_hour 17  
# date\_mday 2  
# date\_minute 60

Generated for () (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 () (C) Splunk Inc, not for distribution

# Make an Interesting Field a Selected Field

- You can modify selected fields

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

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

The screenshot illustrates the process of selecting an interesting field as a selected field. It shows two panels: a sidebar and a main event viewer.

**Left Sidebar:** Shows the "SELECTED FIELDS" section containing "a host 3", "a source 3", and "a sourcetype 1". Below it is the "INTERESTING FIELDS" section, which contains "a action 1", "# bytes 100+", "a categoryId 8", "a clientip 100+", "# date\_hour 18", "# date\_mday 1", "# date\_minute 59", and "a date\_month 1". The "a action 1" field is highlighted with a green box and has a red circle with the number "1" above it, indicating it is the target for selection.

**Right Panel:** Shows event details for "action" on 1/4/18. The event ID is 201.42.223.29 - [04/Jan/2018:17:20:31] "POST /cart/success.do?JSE...". The "action" field has a value of "purchase". A "Selected" checkbox is checked, and a "Yes" button is highlighted with a green box and a red circle with the number "2", indicating it was clicked to confirm the selection.

**Bottom Panel:** Shows a timeline visualization of 392 events from 1/4/18 to 1/5/18. Below the timeline is a table of events. In the "Event" column, the "action = purchase" value is highlighted with a green box.

Generated for () (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 Splunk interface with the 'Select Fields' modal open over a search results page. The 'All Fields' button in the sidebar is highlighted with a green box and an arrow pointing to the 'Select Fields' modal.

**Select Fields**

Select All Within Filter   Deselect All   Coverage: 1% or more ▾   Filter      + Extract New Fields

|   | Field      | # of Values | Event Coverage | Type   |
|---|------------|-------------|----------------|--------|
| > | action     | 1           | 100%           | String |
| > | host       | 3           | 100%           | String |
| > | source     | 3           | 100%           | String |
| > | sourcetype | 1           | 100%           | String |
| > | JSESSIONID | >100        | 100%           | String |
| > | bytes      | >100        | 100%           | Number |
| > | categoryid | 8           | 50.77%         | String |

**Hide Fields**   **All Fields**

**SELECTED FIELDS**

- a action 1
- a host 3
- a source 3
- a sourcetype 1

5:20:31.000 PM 0 915 "http://www.butte Mac OS X 10\_7\_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36" action = purchase host

1/4/18 201.42.223.29 - - [04/J

Generated for () (C) Splunk Inc, not for distribution

# The Field Window

Select a field from the Fields sidebar, then:

Narrow the search to show only results that contain this field  
**action = \*** is added to the search criteria

Get statistical results

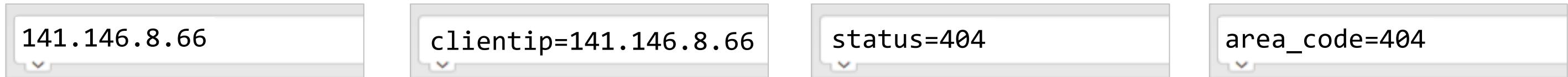
Click a value to add the field/value pair to your search – in this case, **action = addtocart** is added to the search criteria

| Value            | Count | %       |
|------------------|-------|---------|
| failure          | 1,942 | 49.923% |
| view             | 440   | 11.311% |
| purchase         | 392   | 10.077% |
| <b>addtocart</b> | 377   | 9.692%  |
| success          | 230   | 5.912%  |
| TCP_REFRESH_HIT  | 189   | 4.859%  |
| remove           | 100   | 2.602%  |
| TCP_DENIED       | 43    | 1.105%  |

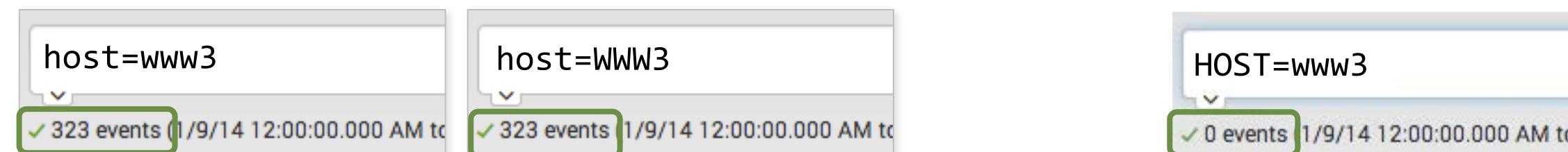
Generated for () (C) Splunk Inc, not for distribution

# Using Fields in Searches

- Efficient way to pinpoint searches and refine results



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



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="202.201.1.0/24"
```

```
clientip="202.201.1.*"
```

- 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
```

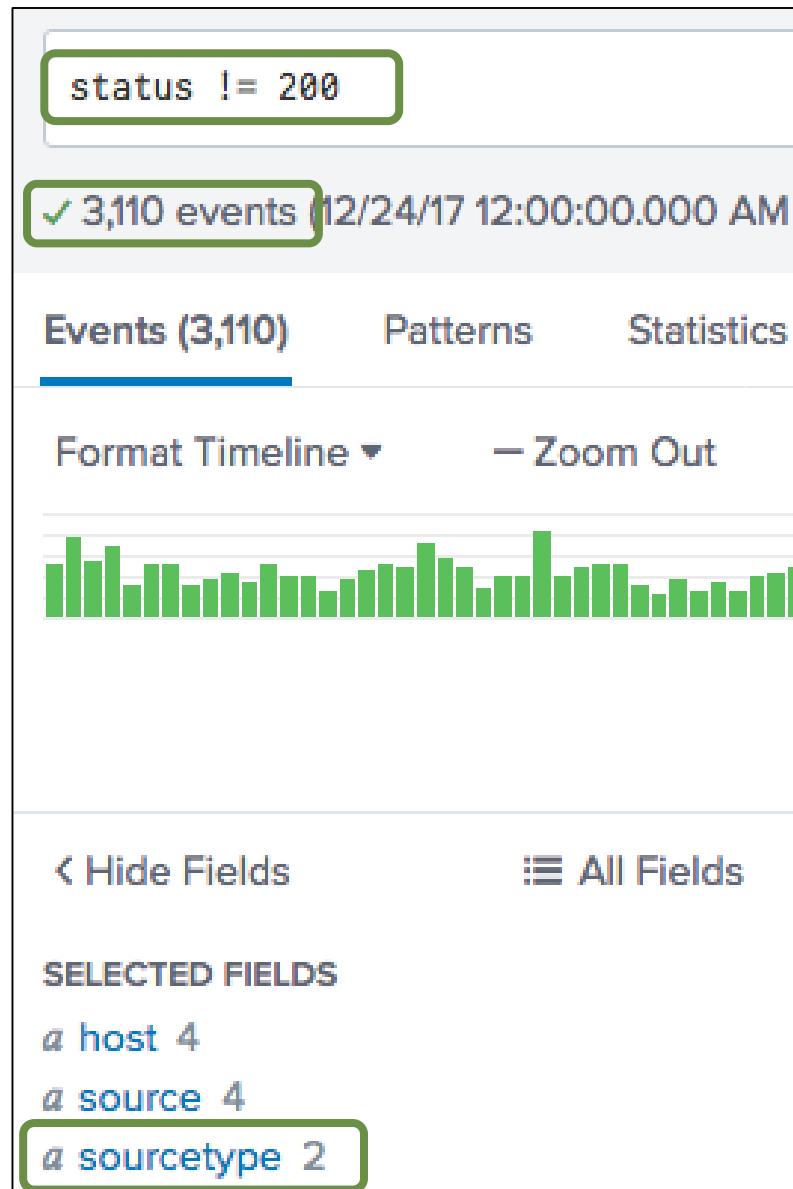
Generated for () (C) Splunk Inc, not for distribution

# `!=` vs. `NOT`

---

- Both `!=` field expression and `NOT` operator exclude events from your search, but produce different results
- Example: `status != 200`
  - Returns events where `status` field exists and value in field doesn't equal 200
- Example: `NOT status = 200`
  - Returns events where `status` field exists and value in field doesn't equal 200 -- **and** all events where `status` field **doesn't** exist

# $\neq$ vs. NOT (cont.)

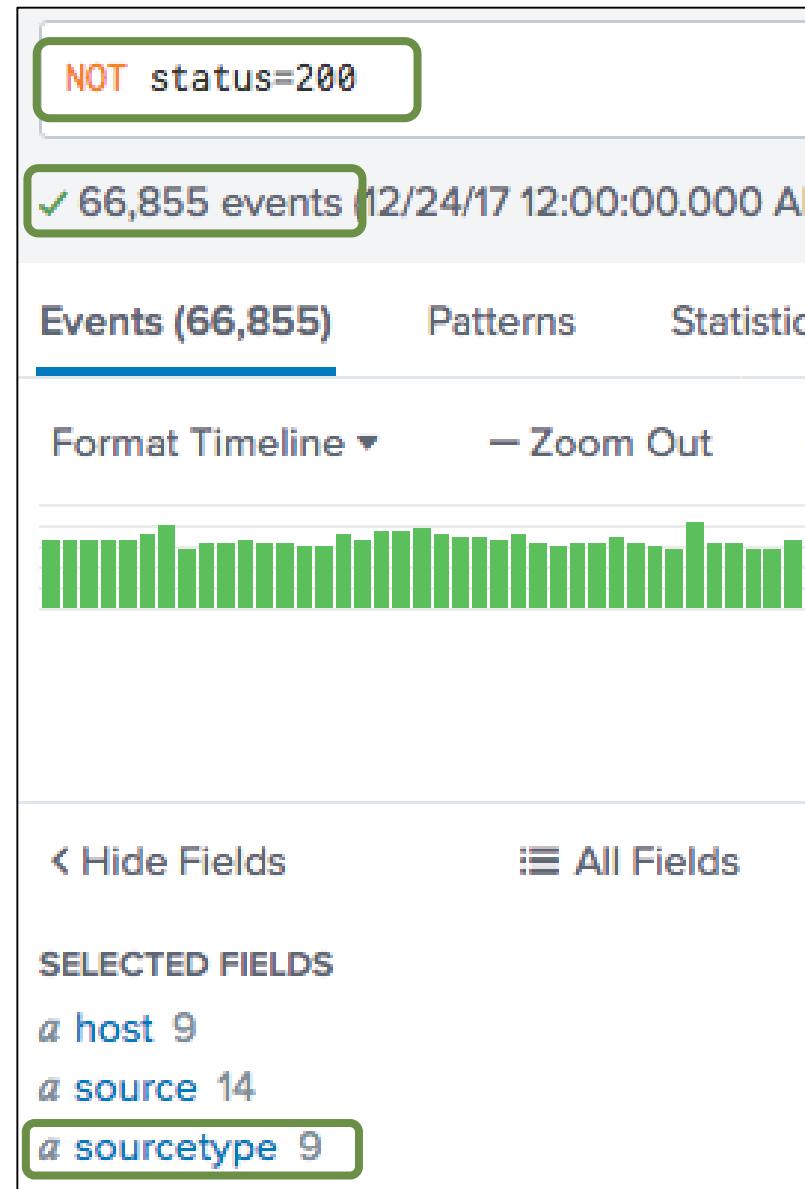


In this example:

- `status != 200` returns **3,110** events from **2** sourcetypes
- `NOT status=200` returns **66,855** events from **9** sourcetypes

### Note

The results from a search using `!=` are a **subset** of the results from a similar search using `NOT`.



Generated for () (C) Splunk Inc, not for distribution

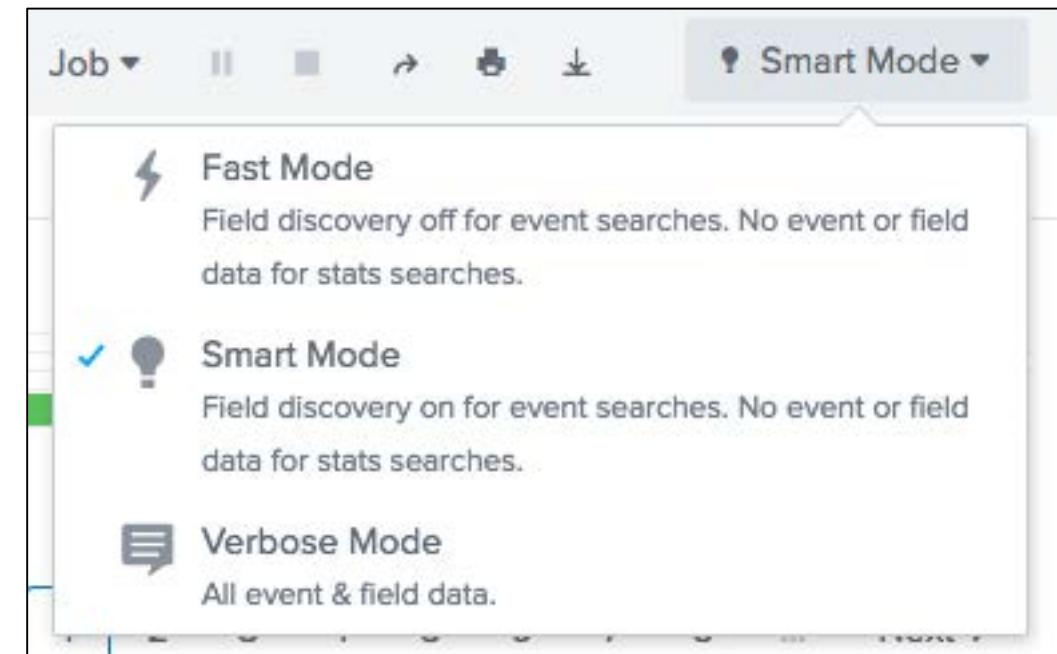
# **!= vs. NOT (cont.)**

---

- Does != and NOT ever yield the same results?
    - Yes, if you know the field you're evaluating always exists in the data you're searching
    - For example:
      - `index=web sourcetype=access_combined status!=200`
      - `index=web sourcetype=access_combined NOT status=200`
- yields same results because status field always exists in access\_combined sourcetype

# Search Modes: Fast, Smart, Verbose

- Fast: emphasizes speed over completeness
- Smart: balances speed and completeness (default)
- Verbose:
  - Emphasizes completeness over speed
  - Allows access to underlying events when using reporting or statistical commands (in addition to totals and stats)



Note

You'll discuss statistical commands later in this course.

# Module 7

# Best Practices

Generated for () (C) Splunk Inc, not for distribution

# Search Best Practices

---

- Time is the most efficient filter
- Specify one or more index values at the beginning of your search string
- Include as many search 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
- Make your search terms as specific as possible
  - Searching for "access denied" is always better than searching for "denied"
- Inclusion is generally better than exclusion
  - Searching for "access denied" is faster than searching for NOT "access granted"

# Search Best Practices (cont.)

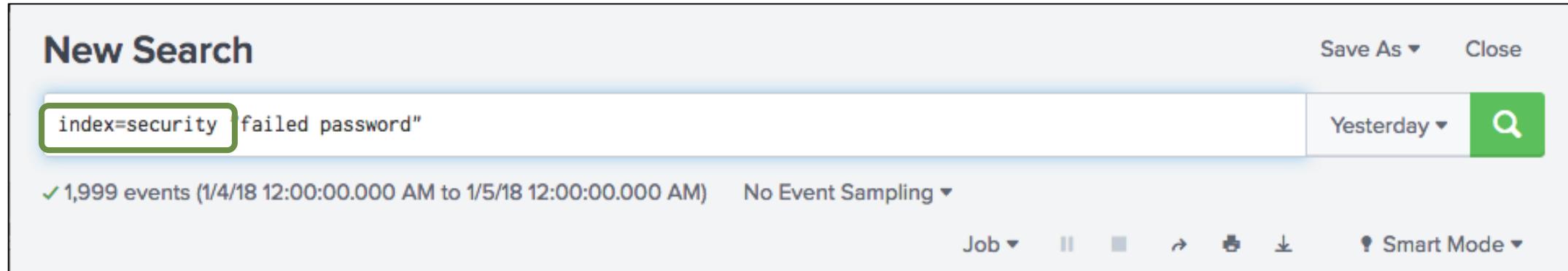
- Filter as early as possible
  - For example, remove duplicate events, then sort
- Avoid using wildcards at the beginning or middle of a string
  - Wildcards at *beginning* of string scan all events within timeframe
  - Wildcards in *middle* of string may return inconsistent results
  - So use fail\* (not \*fail or \*fail\* or f\*il)
- When possible, use OR instead of wildcards
  - For example, use (user=admin **OR** user=administrator) instead of user=admin\*

Note

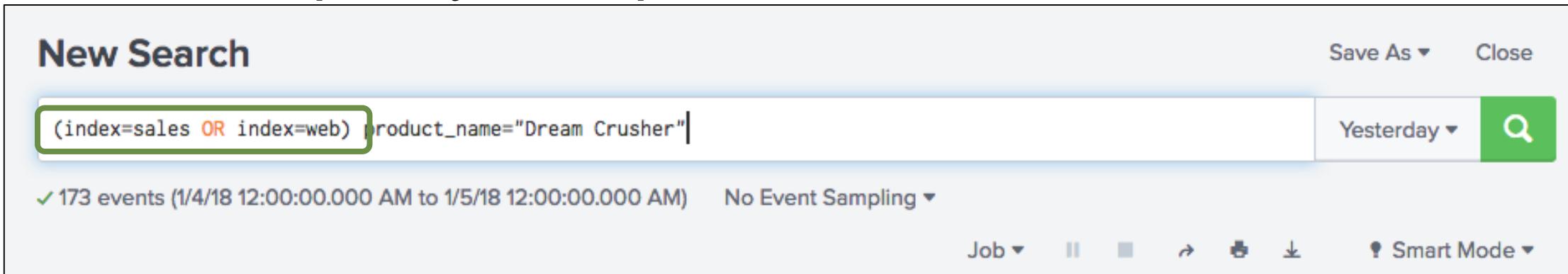
Remember, field names are case *sensitive* and field values are case *insensitive*.

# Working with Indexes

- This search returns event data from the security index



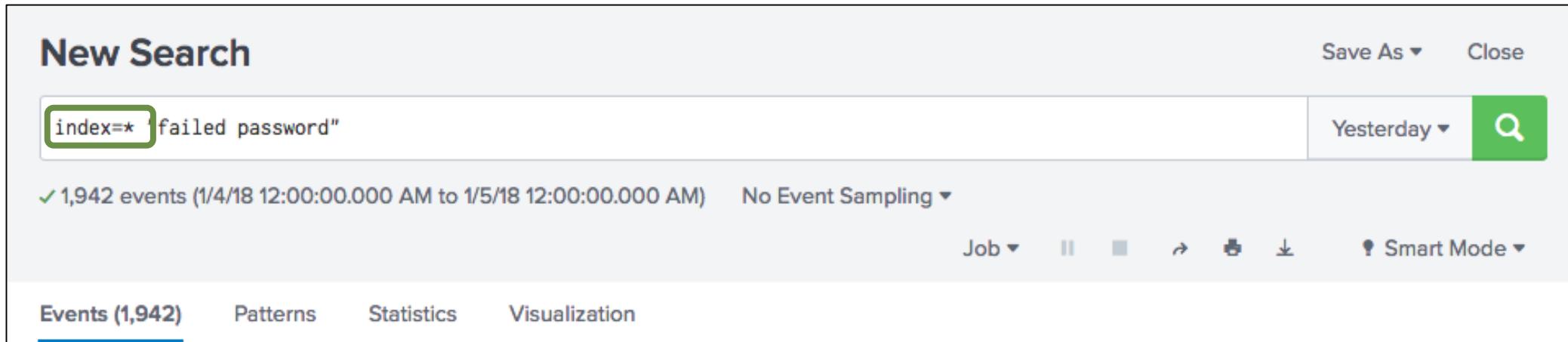
- It's possible to specify multiple index values in a search



Generated for () (C) Splunk Inc, not for distribution

# Working with Indexes (cont.)

- It's possible to use a wildcard (\*) in index values



- It's also possible to search *without* an index—but that's inefficient and **not recommended**

**Note 1** i

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

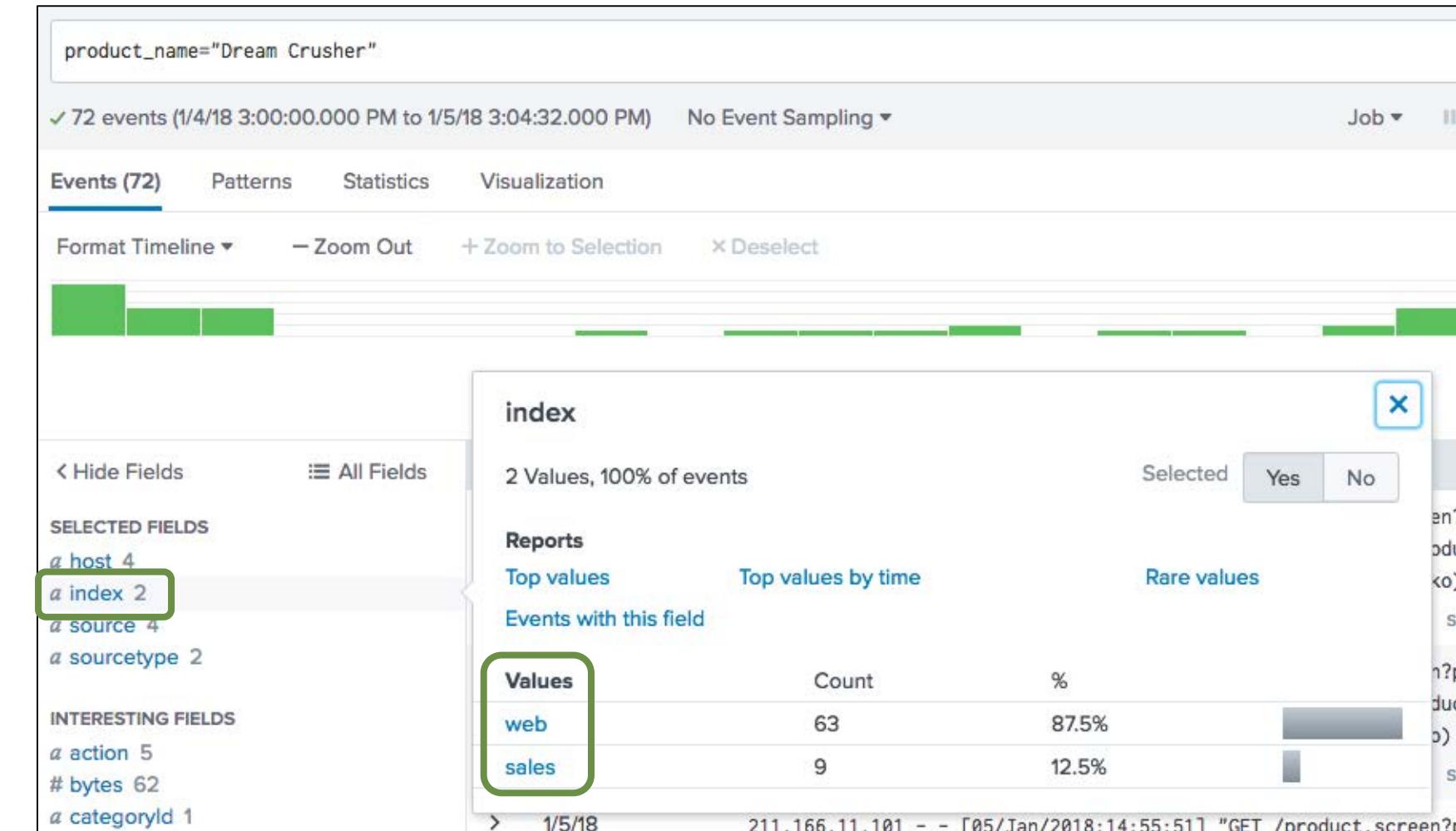
**Note 2** i

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

Generated for () (C) Splunk Inc, not for distribution

# Viewing the Index Field

- The *index* always appears as a field in search results
- In the search shown here, no index was indicated in the search, so data is returned from two indexes: web and sales
- Remember, this practice is **not** recommended—it's always more efficient to specify one or more indexes in your search



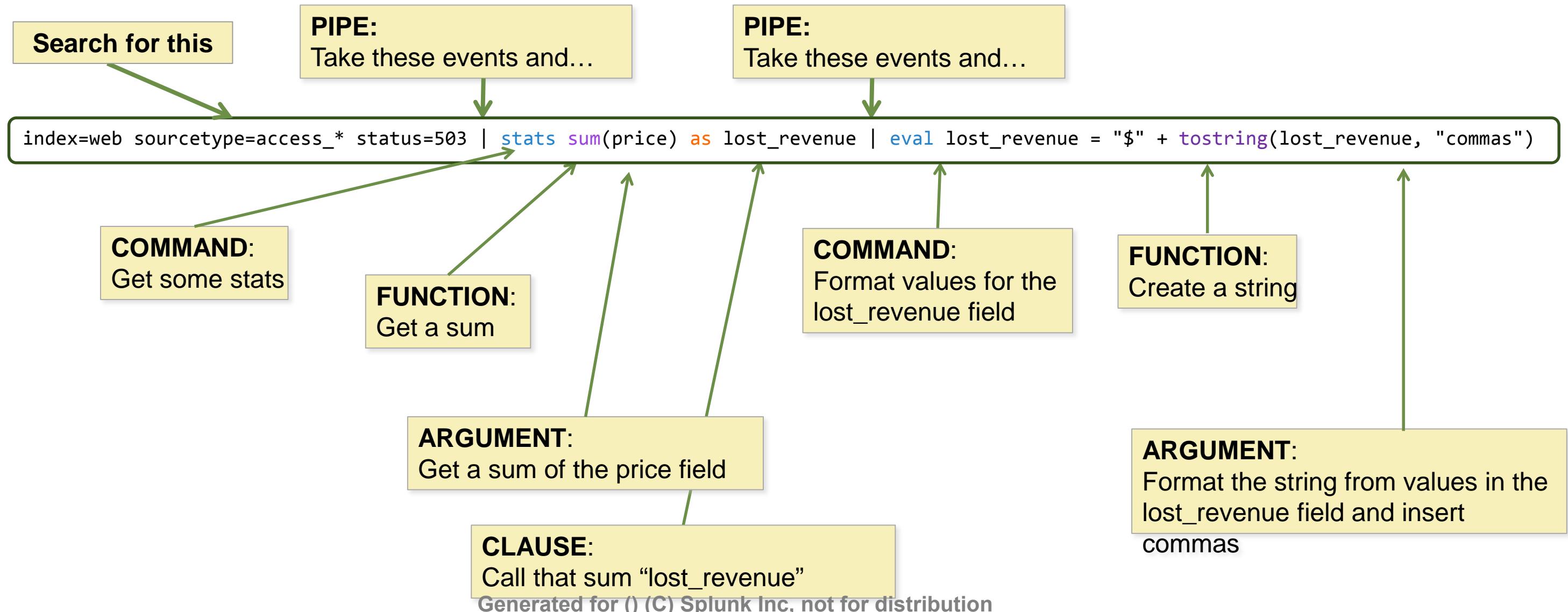
Generated for () (C) Splunk Inc, not for distribution

# Module 8: Splunk's Search Language

Generated for () (C) Splunk Inc, not for distribution

# Search Language Syntax

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

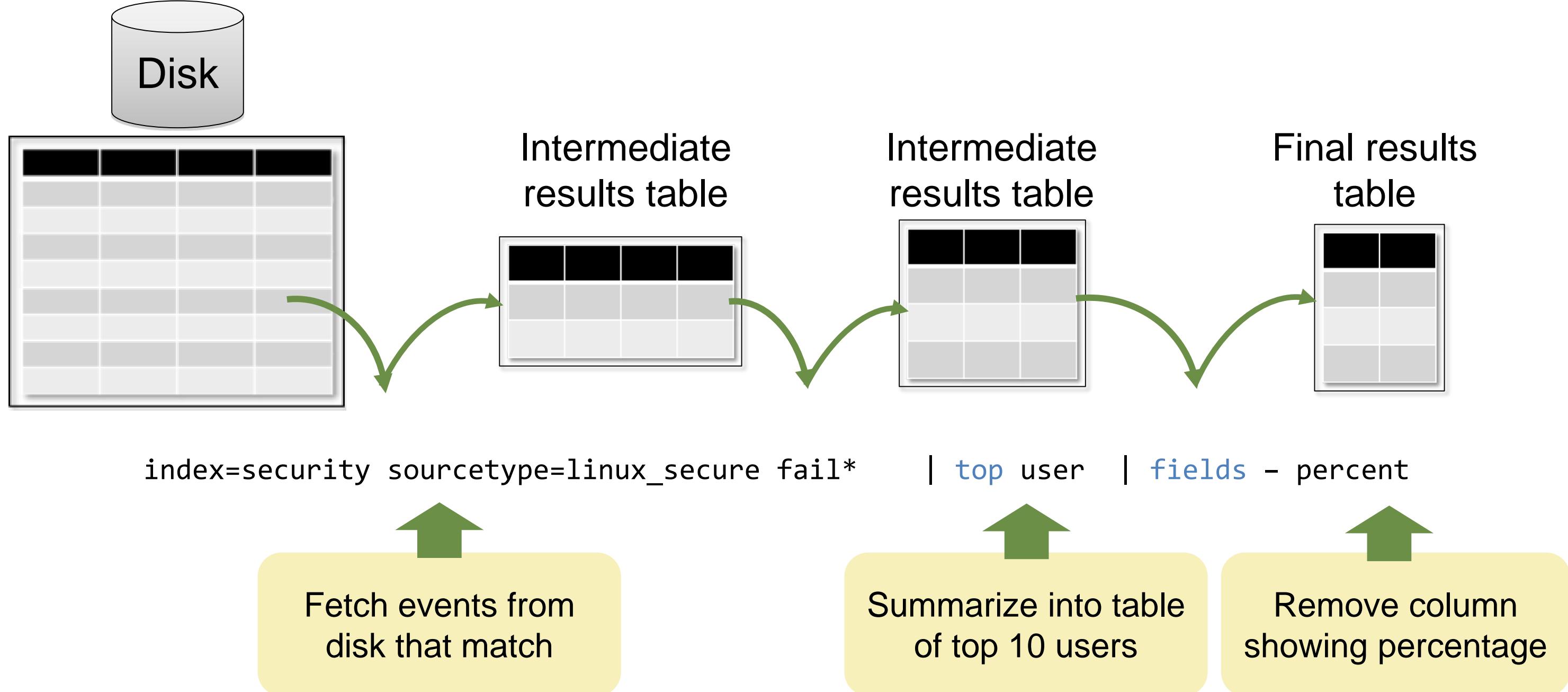


# Search Language Syntax Components

---

- Searches are made up of 5 basic components
  1. **Search terms** – what are you looking for?
    - Keywords, phrases, Booleans, etc.
  2. **Commands** – what do you want to do with the results?
    - Create a chart, compute statistics, evaluate and format, etc.
  3. **Functions** – how do you want to chart, compute, or evaluate the results?
    - Get a sum, get an average, transform the values, etc.
  4. **Arguments** – are there variables you want to apply to this function?
    - Calculate average value for a specific field, convert milliseconds to seconds, etc.
  5. **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



# Making the Pipeline More Readable

- Put each pipe in the pipeline on a separate line as you type by turning on auto-formatting
- Go to **Preferences > SPL Editor** and turn on Search auto-format

Instead of this:

New Search

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

You'll get this:

New Search

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

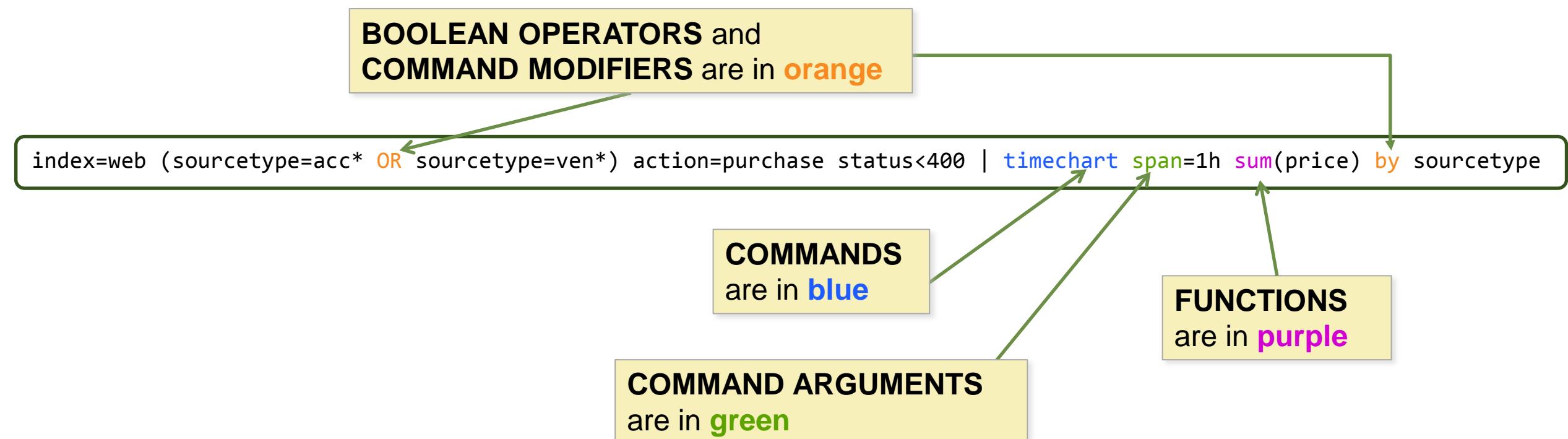
Note 

You can also use **Shift + Enter** to go to a new line.

Generated for () (C) Splunk Inc, not for distribution

# Syntax Coloring

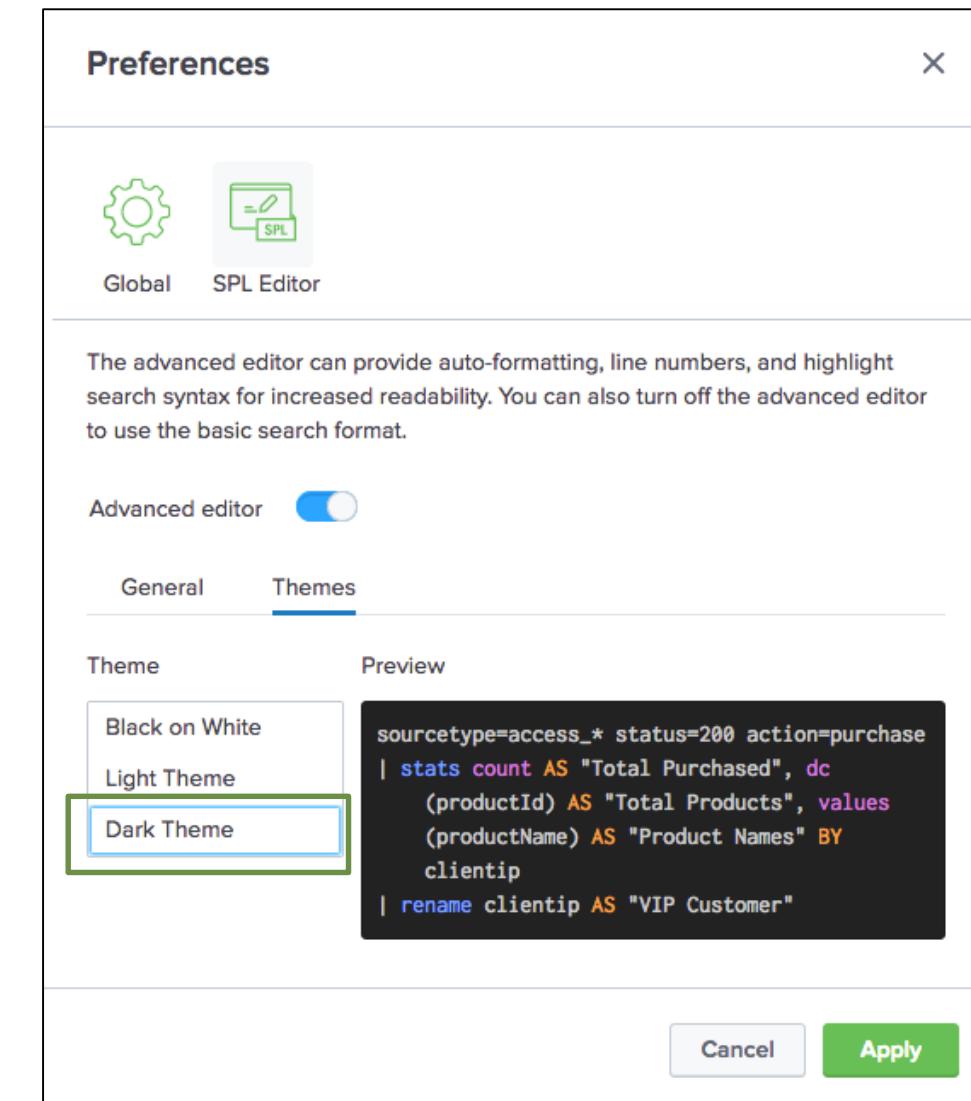
- By default, some parts of the search string are automatically colored as you type
- The color is based on the search syntax
- The rest of the search string remains black



Generated for () (C) Splunk Inc, not for distribution

# Syntax Coloring (cont.)

- You can turn off automatic syntax coloring
  1. Go to **Preferences > SPL Editor**
  2. Choose the Themes tab and select Black on White instead of the Light Theme default
  3. Click Apply
- You can also display colored text against a black background by selecting Dark Theme



```
index=web (sourcetype=acc* OR sourcetype=ven*) action=purchase status<400 | timechart span=1h sum(price) by sourcetype
```

Generated for () (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 represents an event
  - Each row contains field values for that event

## 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 |
|-----------------|-----------|-----------|--------|
| 220.225.12.171  | view      | WC-SH-A02 | 200    |
| 220.225.12.171  |           | WC-SH-G04 | 200    |
| 188.173.152.100 |           | CU-PG-G06 | 200    |
| 188.173.152.100 | purchase  |           | 200    |
| 188.173.152.100 | purchase  | WC-SH-T02 | 200    |
| 188.173.152.100 | addtocart | WC-SH-T02 | 200    |
| 188.173.152.100 |           | WC-SH-T02 | 200    |
| 188.173.152.100 |           | WC-SH-A02 | 200    |

Generated for () (C) Splunk Inc, not for distribution

# Renaming Fields in a Table

- 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
| rename action as "Customer Action", B
| rename status as "HTTP Status" C
```

| clientip     | Customer Action | ProductID | HTTP Status |
|--------------|-----------------|-----------|-------------|
| 12.130.60.4  |                 |           | 200         |
| 27.102.11.11 |                 | SC-MG-G10 | 200         |
| 27.102.11.11 |                 | DC-SG-G02 | 200         |
| 27.102.11.11 |                 |           | 200         |
| 27.102.11.11 | view            | FI-AG-G08 | 200         |
| 99.61.68.230 | purchase        |           | 200         |
| 99.61.68.230 | purchase        | WC-SH-A01 | 200         |
| 99.61.68.230 | addtocart       | WC-SH-A01 | 200         |

Generated for () (C) Splunk Inc, not for distribution

# Renaming Fields in a Table (cont.)

Once you rename a field, you can't access it with the original name

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

No results found.

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

| Customer Action | HTTP Status |
|-----------------|-------------|
| purchase        | 200         |
| purchase        | 200         |
| addtocart       | 200         |
|                 | 200         |
|                 | 200         |
| view            | 200         |
| view            | 200         |
|                 | 200         |

Generated for () (C) Splunk Inc. not for distribution

# Using the 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

Generated for () (C) Splunk Inc, not for distribution

# fields Command – Examples

Using command improves performance—only specified fields extracted

Scenario ?

Display network failures during the previous week.

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

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

| < Hide Fields      |   | All Fields | i | Time                      | Event   |
|--------------------|---|------------|---|---------------------------|---|
| SELECTED FIELDS    |   |            | > | 1/6/18<br>11:58:24.000 PM | Sat Jan 06 2018 23:58:24 www3 sshd[4559]: Failed password for nagios from 67.133.102.<br>54 port 4437 ssh2<br>host = www3   source = /opt/log/www3/secure.log   sourcetype = linux_secure               |
| a host             | 4 |            | > | 1/6/18<br>11:58:24.000 PM | Sat Jan 06 2018 23:58:24 mailsv1 sshd[1258]: Failed password for myuan from 77.123.10<br>2.237 port 1611 ssh2<br>host = mailsv1   source = /opt/log-mailsv1/secure.log   sourcetype = linux_secure      |
| a source           | 4 |            | > | 1/6/18<br>11:58:24.000 PM | Sat Jan 06 2018 23:58:24 www2 sshd[1896]: Failed password for nagios from 87.194.216.<br>51 port 3698 ssh2<br>host = www2   source = /opt/log/www2/secure.log   sourcetype = linux_secure               |
| a sourcetype       | 1 |            | > | 1/6/18<br>11:58:24.000 PM | Sat Jan 06 2018 23:58:24 www3 sshd[2746]: Failed password for invalid user db2dba fro<br>m 203.45.206.135 port 3825 ssh2<br>host = www3   source = /opt/log/www3/secure.log   sourcetype = linux_secure |
| INTERESTING FIELDS |   |            |   |                           |   |
| a action           | 1 |            |   |                           |   |
| a app              | 1 |            |   |                           |   |

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 | Time                      | Event  |
|----------------------|------|------------|---|---------------------------|--|
| INTERESTING FIELDS   |      |            | > | 1/6/18<br>11:58:24.000 PM | Sat Jan 06 2018 23:58:24 www3 sshd[4559]: Failed password for nagios from 67.133.102.<br>54 port 4437 ssh2               |
| a app                | 1    |            | > | 1/6/18<br>11:58:24.000 PM | Sat Jan 06 2018 23:58:24 mailsv1 sshd[1258]: Failed password for myuan from 77.123.10<br>2.237 port 1611 ssh2            |
| a src_ip             | 100+ |            | > | 1/6/18<br>11:58:24.000 PM | Sat Jan 06 2018 23:58:24 www2 sshd[1896]: Failed password for nagios from 87.194.216.<br>51 port 3698 ssh2               |
| a user               | 100+ |            | > | 1/6/18<br>11:58:24.000 PM | Sat Jan 06 2018 23:58:24 www3 sshd[2746]: Failed password for invalid user db2dba fro<br>m 203.45.206.135 port 3825 ssh2 |
| + Extract New Fields |      |            |   |                           |  |

Generated for () (C) Splunk Inc, not for distribution

# Using the dedup Command

Use dedup to remove duplicates from your results

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

| Vendor         | VendorCity      | VendorStateProvince | VendorCountry |
|----------------|-----------------|---------------------|---------------|
| Beach Games    | Miami           | Florida             | United States |
| Beads & Games  | Ft. Riley       | Kansas              | United States |
| Beach Games    | Miami           | Florida             | United States |
| Beantown Games | Boston          | Massachusetts       | United States |
| Beantown Games | Boston          | Massachusetts       | United States |
| Beach Games    | Fort Lauderdale | Florida             | United States |

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

| Vendor         | VendorCity | VendorStateProvince | VendorCountry |
|----------------|------------|---------------------|---------------|
| Beach Games    | Miami      | Florida             | United States |
| Beads & Games  | Ft. Riley  | Kansas              | United States |
| Beantown Games | Boston     | Massachusetts       | United States |
| Beauty Games   | Butte      | Montana             | United States |

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

| Vendor         | VendorCity      | VendorStateProvince | VendorCountry |
|----------------|-----------------|---------------------|---------------|
| Beach Games    | Miami           | Florida             | United States |
| Beads & Games  | Ft. Riley       | Kansas              | United States |
| Beach Games    | Fort Lauderdale | Florida             | United States |
| Beantown Games | Boston          | Massachusetts       | United States |
| Beauty Games   | Butte           | Montana             | United States |

Generated for () (C) Splunk Inc, not for distribution

# Using the 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 ↗](#)

# Using the 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
Vendor=Bea*
| dedup Vendor, VendorCity
| table Vendor, VendorCity,
VendorStateProvince, VendorCountry
| sort -Vendor, VendorCity
```

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

| Vendor         | VendorCity      | VendorStateProvince | VendorCountry |
|----------------|-----------------|---------------------|---------------|
| Beauty Games   | Butte           | Montana             | United States |
| Beantown Games | Boston          | Massachusetts       | United States |
| Beads & Games  | Ft. Riley       | Kansas              | United States |
| Beach Games    | Fort Lauderdale | Florida             | United States |
| Beach Games    | Miami           | Florida             | United States |

| Vendor         | VendorCity      | VendorStateProvince | VendorCountry |
|----------------|-----------------|---------------------|---------------|
| Beauty Games   | Butte           | Montana             | United States |
| Beantown Games | Boston          | Massachusetts       | United States |
| Beads & Games  | Ft. Riley       | Kansas              | United States |
| Beach Games    | Miami           | Florida             | United States |
| Beach Games    | Fort Lauderdale | Florida             | United States |

Generated for () (C) Splunk Inc, not for distribution

# Useful References

---

- Search Reference:

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

- Search Quick Reference:

<http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/SplunkEnterpriseQuickReferenceGuide>

# Module 9

# Transforming Commands

Generated for () (C) Splunk Inc, not for distribution

# Getting Top Values

- The top command finds the most common values of a given field in the result set
- By default, output displays in table format

| src_ip         | count | percent   |
|----------------|-------|-----------|
| 132.55.227.221 | 105   | 27.131783 |
| 214.156.206.45 | 9     | 2.325581  |
| 118.6.85.68    | 9     | 2.325581  |
| 87.194.216.51  | 8     | 2.067183  |
| 108.65.113.83  | 6     | 1.550388  |
| 89.11.192.18   | 5     | 1.291990  |
| 211.166.11.101 | 5     | 1.291990  |
| 195.69.160.22  | 5     | 1.291990  |
| 81.18.148.190  | 4     | 1.033592  |
| 223.205.219.67 | 4     | 1.033592  |

## Scenario

Determine which IP addresses generated the most attacks in the last 60 minutes,

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

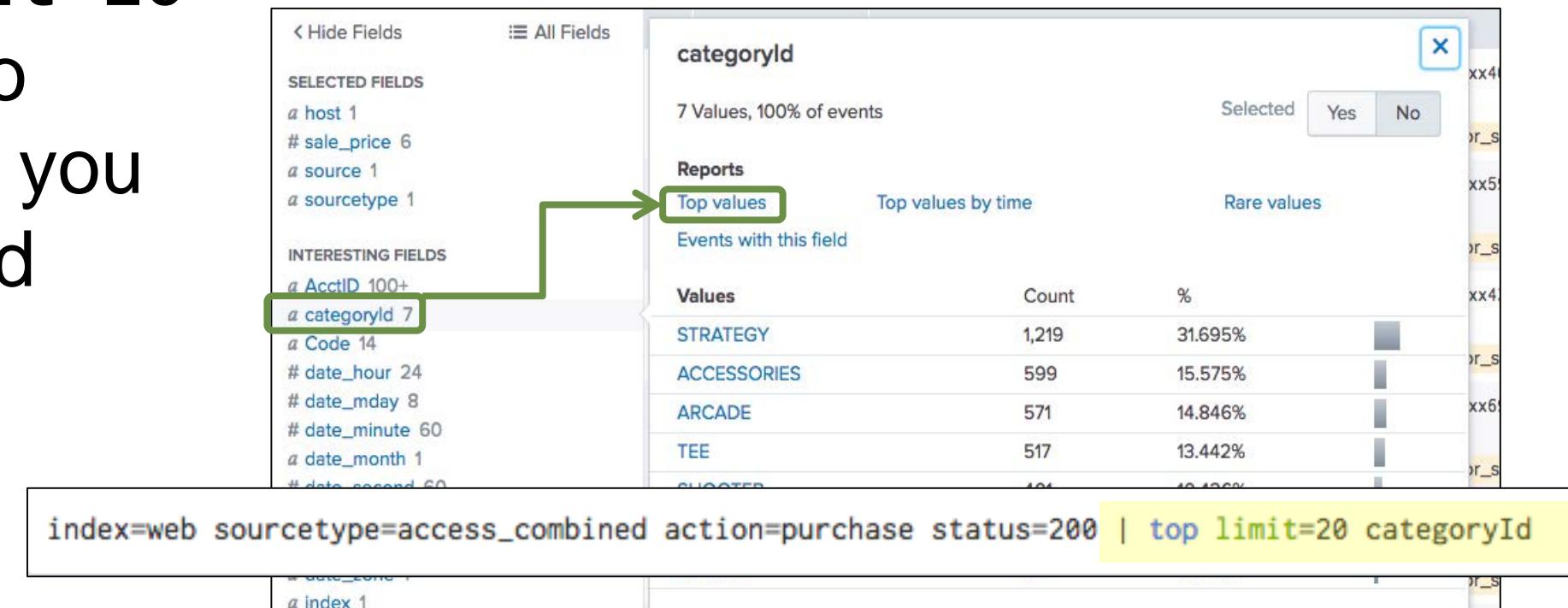
Generated for () (C) Splunk Inc, not for distribution

# top Command

- By default, returns top 10 results
- Automatically returns count and percent columns
- Common constraints: limit countfield showperc
- top command with limit=20 is automatically added to your search string when you click Top values in a field window

Note

Creating top values reports from field windows was discussed in Module 4.



Generated for () (C) Splunk Inc. not for distribution

# top Command – Single Field

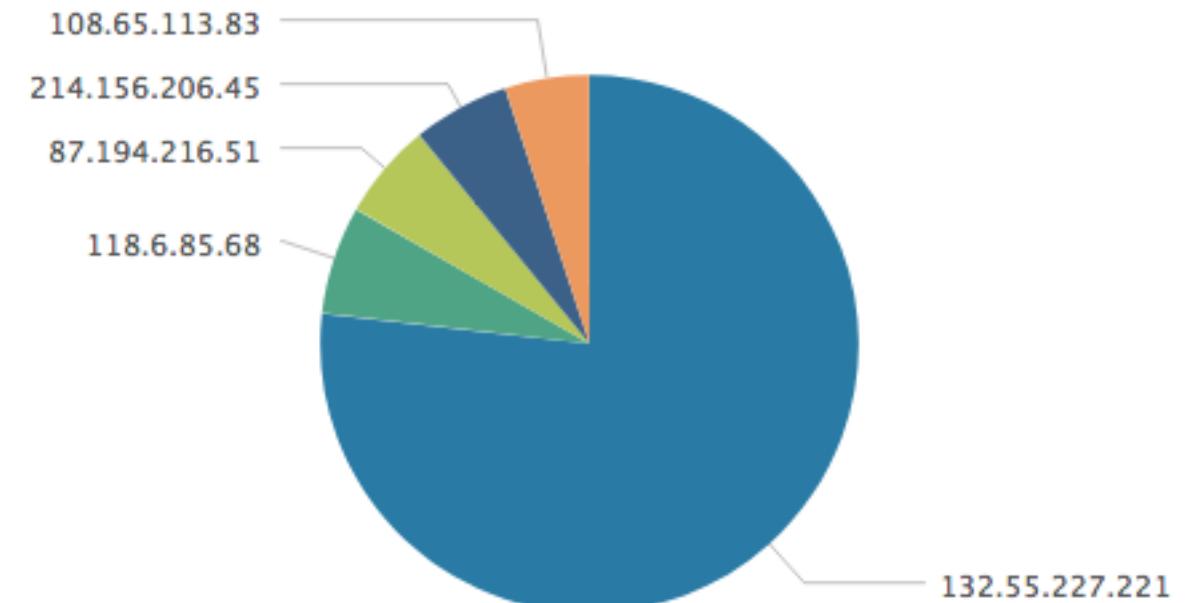
- Control # of results displayed using `limit`
- `limit=#` returns this number of results
- `limit=0` returns unlimited results

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

Scenario ?

During the last hour, display the top 5 IPs that generated the most attacks.

| src_ip         | count | percent   |
|----------------|-------|-----------|
| 132.55.227.221 | 106   | 27.390181 |
| 118.6.85.68    | 9     | 2.325581  |
| 87.194.216.51  | 8     | 2.067183  |
| 214.156.206.45 | 8     | 2.067183  |
| 108.65.113.83  | 7     | 1.808786  |



Generated for () (C) Splunk Inc, not for distribution

# top Command – Multiple Fields

- 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 cs_username A x_webcat_code_full limit=3 B
```

| cs_username                 | x_webcat_code_full     | count | percent  |
|-----------------------------|------------------------|-------|----------|
| kjoslin@buttercupgames.com  | Sports and Recreation  | 81    | 6.617647 |
| kperna@buttercupgames.com   | Shopping               | 61    | 4.983660 |
| apreusig@buttercupgames.com | Arts and Entertainment | 58    | 4.738562 |

Generated for () (C) Splunk Inc, not for distribution

**splunk**® listen to your data®

116

Splunk Fundamentals 1  
Copyright © 2018 Splunk, Inc. All rights reserved | 24 May 2018

# top Command – Single Field with by Clause

## Scenario 1



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

```
index=network sourcetype=cisco_wsa_squid  
| top x_webcat_code_full by cs_username limit=3
```

B

A

| cs_username                    | x_webcat_code_full     | count | percent   |
|--------------------------------|------------------------|-------|-----------|
| acurry@buttercupgames.com      | Uncategorized URLs     | 5     | 35.714286 |
| acurry@buttercupgames.com      | Shopping               | 4     | 28.571429 |
| acurry@buttercupgames.com      | Health and Nutrition   | 3     | 21.428571 |
| adombrowski@buttercupgames.com | Uncategorized URLs     | 1     | 50.000000 |
| adombrowski@buttercupgames.com | Computers and Internet | 1     | 50.000000 |
| apreusig@buttercupgames.com    | Arts and Entertainment | 58    | 95.081967 |

A

B

```
index=network sourcetype=cisco_wsa_squid  
| top cs_username by x_webcat_code_full limit=3
```

C

D

| x_webcat_code_full     | cs_username                   | count | percent   |
|------------------------|-------------------------------|-------|-----------|
| Advertisements         | gnooteboom@buttercupgames.com | 5     | 41.666667 |
| Advertisements         | iking@buttercupgames.com      | 3     | 25.000000 |
| Advertisements         | tzielinski@buttercupgames.com | 2     | 16.666667 |
| Arts and Entertainment | fbryan@buttercupgames.com     | 61    | 46.923077 |
| Arts and Entertainment | moh@buttercupgames.com        | 6     | 4.615385  |
| Arts and Entertainment | pbunch@buttercupgames.com     | 4     | 3.076923  |

D

C

Generated for () (C) Splunk Inc, not for distribution

# top Command – Renaming countfield Display

- By default, the display name of the countfield is count
- `countfield=string` renames the field for display purposes

**Scenario** ?

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

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

| cs_username                 | x_webcat_code_full      | Total Viewed |
|-----------------------------|-------------------------|--------------|
| kjoslin@buttercupgames.com  | A Sports and Recreation | B 81         |
| kperna@buttercupgames.com   | Shopping                | 61           |
| apreusig@buttercupgames.com | Arts and Entertainment  | 58           |

**Note** i

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

Generated for () (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 ?

Identify 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
```



Generated for () (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 () (C) Splunk Inc, not for distribution

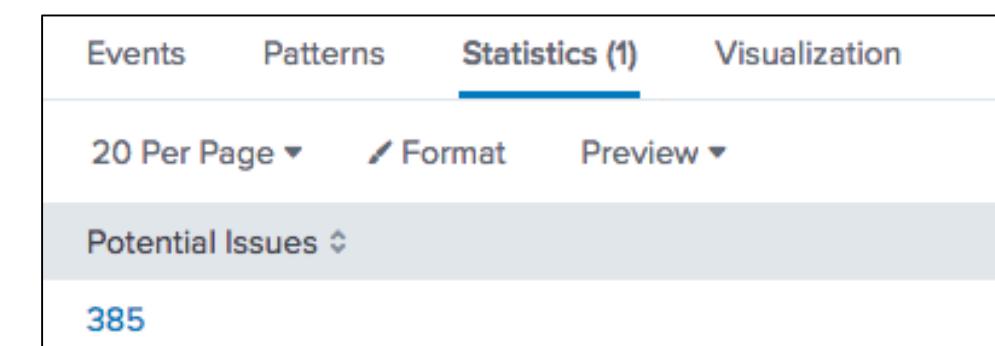
# stats Command – count

- 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"
```



Generated for () (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 () (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 |
|---------------|------|---------------|-------|
| administrator | sshd | Failed        | 1     |
| agushto       | sshd | Failed        | 1     |
| backup        | sshd | Failed        | 1     |
| bin           | sshd | Failed        | 2     |
| brian         | sshd | Failed        | 1     |
| db            | sshd | Failed        | 2     |
| db2fenc1      | sshd | Failed        | 2     |
| db4           | sshd | Failed        | 1     |
| dba           | sshd | Failed        | 1     |
| demon         | sshd | Failed        | 1     |

Generated for () (C) Splunk Inc, not for distribution

# 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 employees visited in the last 4 hours?

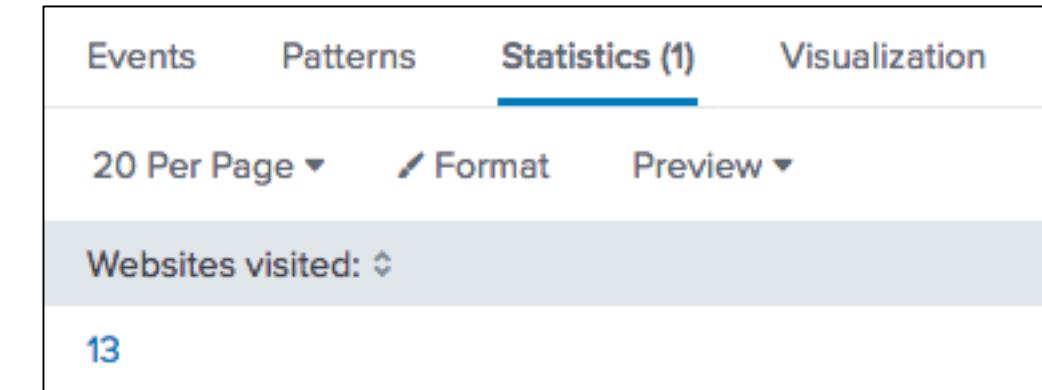
```
index=network sourcetype=cisco_wsa_squid  
| stats dc(s_hostname) as "Websites visited:"
```

Events Patterns Statistics (1) Visualization

20 Per Page ▾ Format Preview ▾

Websites visited: ▾

13

A screenshot of a Splunk search interface. At the top, there are tabs for 'Events', 'Patterns', 'Statistics (1)', and 'Visualization'. The 'Statistics (1)' tab is selected. Below the tabs, there are dropdown menus for '20 Per Page' and 'Format', and a 'Preview' button. A search bar contains the query 'Websites visited:'. The results section shows a single row with the value '13'.

# stats Command – sum(*field*)

Scenario ?

How much bandwidth did employees consume 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

A      B      C

| Events              |           | Patterns | Statistics (520) | Visualization |
|---------------------|-----------|----------|------------------|---------------|
| 20 Per Page ▾       |           | Format   | Preview ▾        |               |
| s_hostname          | Bandwidth |          |                  |               |
| www.archerytalk.com | 6330733   |          |                  |               |
| www.infoblox.com    | 2818279   |          |                  |               |
| www.bjc-aces.com    | 1849884   |          |                  |               |
| www.bradblog.com    | 1489356   |          |                  |               |
| www.ncsl.org        | 1425778   |          |                  |               |

Generated for () (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 78       | B 3119.22   |
| World of Cheese     | 78         | 1949.22     |
| Manganiello Bros.   | 45         | 1799.55     |
| SIM Cubicle         | 72         | 1439.28     |
| Final Sequel        | 55         | 1374.45     |
| Mediocre Kingdoms   | 50         | 1249.50     |
| Orvil the Wolverine | 30         | 1199.70     |
| Benign Space Debris | 31         | 774.69      |
| Curling 2014        | 28         | 559.72      |
| World of Cheese Tee | 47         | D 469.53    |

Generated for () (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 | 18870.117341640707 |
| Business   | 12957.355321020228 |
| Personal   | 12915.358326596604 |
| Unknown    | 12747.842960288808 |
| Violation  | 8831.088888888889  |

B

A

Generated for () (C) Splunk Inc, not for distribution

# 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
    - ▶ The same hostname appears 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:   |
|-----------------------------|---|
| apucci@buttercupgames.com   | www.filmschoolrejects.com<br>www.zimbio.com   |
| arangel@buttercupgames.com  | www.cnet.com  |
| basselin@buttercupgames.com | www.americangangster.net<br>www.americangangster.net<br>www.americangangster.net<br>www.blossomfloristla.com<br>84654321.cn |
| bgenin@buttercupgames.com   | www.ambrosiasw.com<br>www.ambrosiasw.com<br>www.ambrosiasw.com  |

Generated for () (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
```

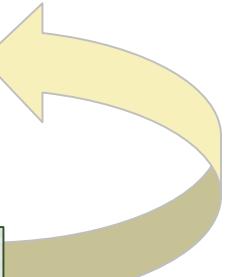
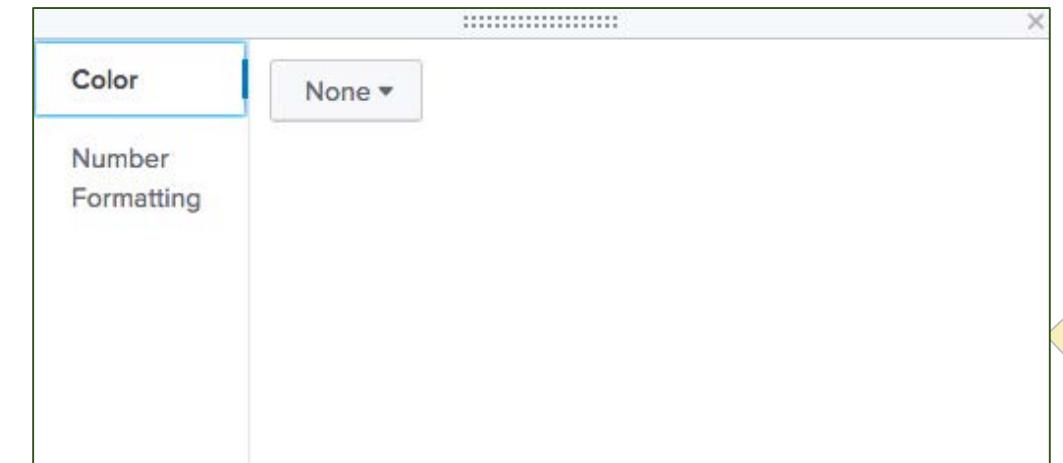
values function lists unique values for the specified field

| src_ip         | User Names                       | Attempts |
|----------------|----------------------------------|----------|
| 107.3.146.207  | administrator<br>pat<br>uni      | 3        |
| 109.169.32.135 | harrypotter<br>irc               | 2        |
| 110.138.30.229 | daemon                           | 1        |
| 111.161.27.20  | administrator<br>daemon<br>games | 3        |
| 112.111.162.4  | noone                            | 1        |

Generated for () (C) Splunk Inc, not for distribution

# Formatting stats Tables

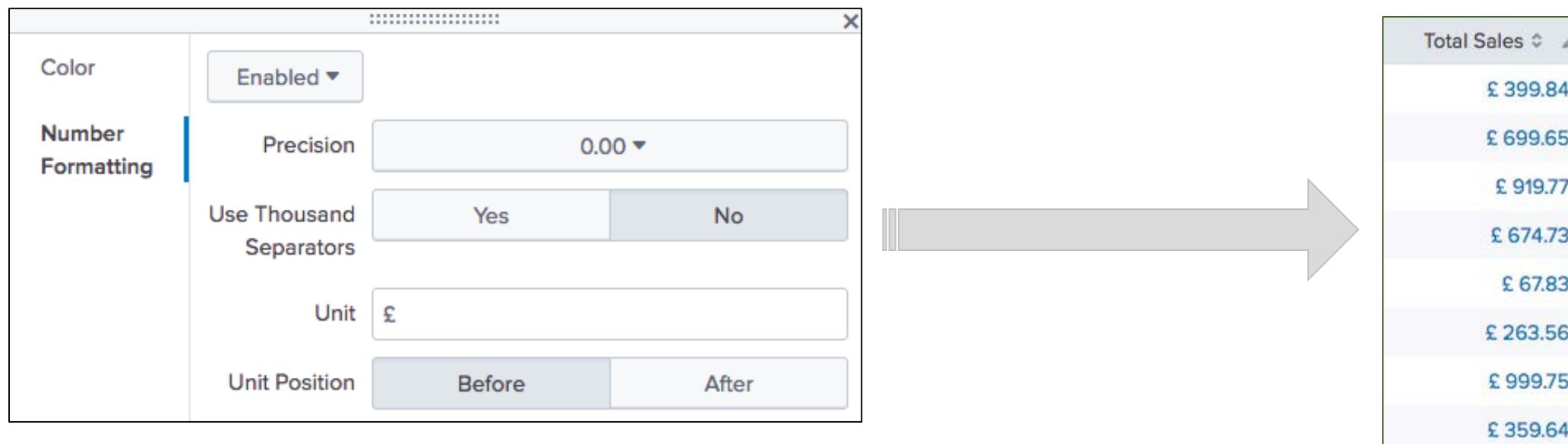
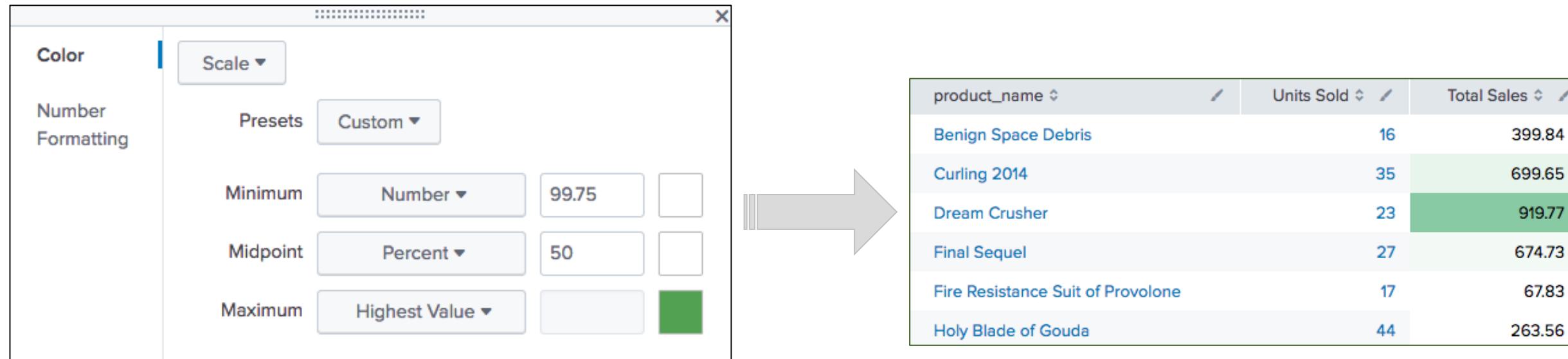
- Tables created with stats commands can be formatted
- Color code data in each column, based on rules you define
- Add number formatting (e.g. currency symbols, thousands separators)
- Can also format data on a per-column basis by clicking the  icon above that column



| product_name        | Units Sold | Total Sales |
|---------------------|------------|-------------|
| Benign Space Debris | 16         | 399.84      |
| Curling 2014        | 35         | 699.65      |
| Dream Crusher       | 23         | 919.77      |
| Final Sequel        | 27         | 674.73      |

Generated for () (C) Splunk Inc, not for distribution

# Formatting stats Tables – Examples



Generated for () (C) Splunk Inc, not for distribution

# Module 10: Creating Reports and Dashboards

Generated for () (C) Splunk Inc, not for distribution

# What Are 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

# 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/Developnamingconventionsforknowledgeobjecttitles>

# Creating a Report from a Search

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

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

- 1 Run a search: The search bar at the top contains the query `index=web sourcetype=access_combined action=purchase status!=200`.
- 2 Select Save As: A context menu is open, with the "Report" option highlighted.
- 3 Select Report: The "Report" option in the context menu is selected.

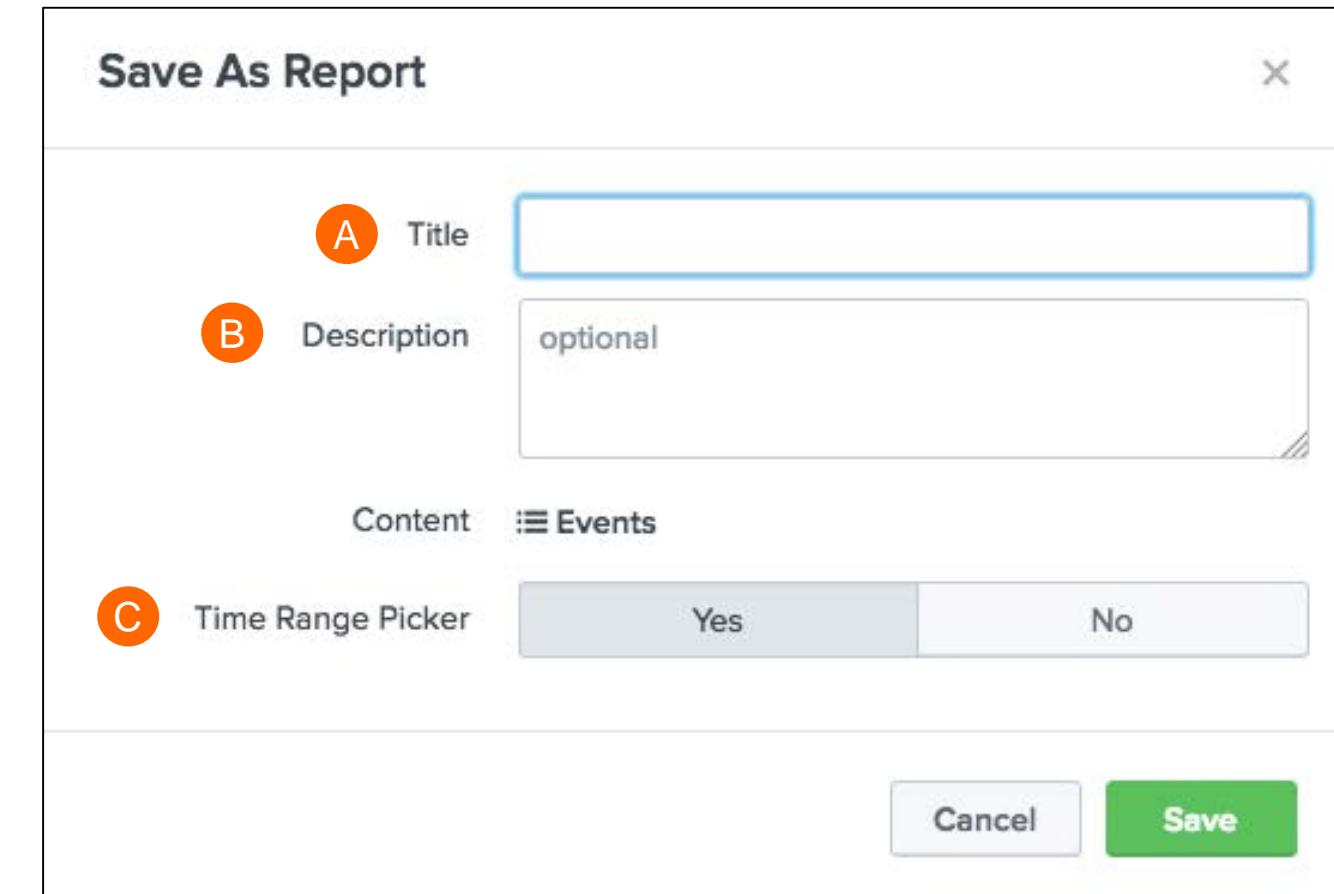
The main search results table displays 50 events from March 11, 2018, to March 12, 2018. The table includes columns for Time, Event, and selected fields (action, host, source, sourcetype). The event details show a Googlebot request for a purchase action.

| i | Time                      | Event  |
|---|---------------------------|--|
| > | 3/12/18<br>6:09:24.000 PM | 81.11.191.113 - - [12/Mar/2018:18:09:24] "POST /cart.do?action=purchase&itemId=EST-17&JSESSIONID=SD10SL9FF5ADFF4963 HTTP/1.1" 503 2768 "http://www.buttercupgames.com/cart.do?acti<br>on=addtocart&itemId=EST-17&categoryId=ARCADE&productId=MB-AG-G07" "Googlebot/2.1 (http://<br>www.googlebot.com/bot.html)" 846<br>action = purchase   host = www1   source = /opt/log/www1/access.log |

Generated for () (C) Splunk Inc, not for distribution

# Creating a Report from a Search (cont.)

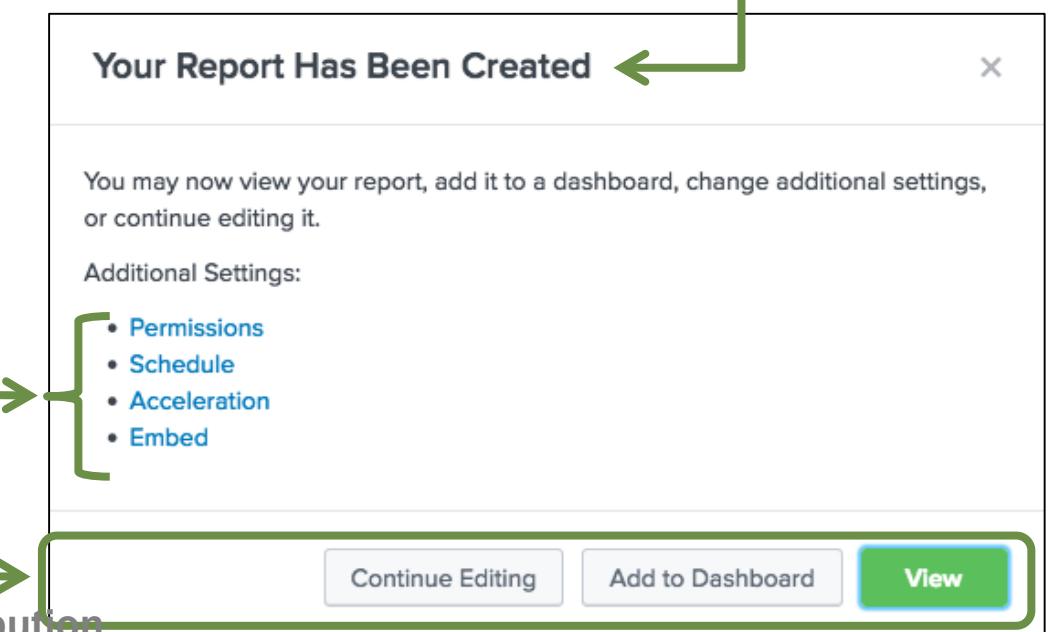
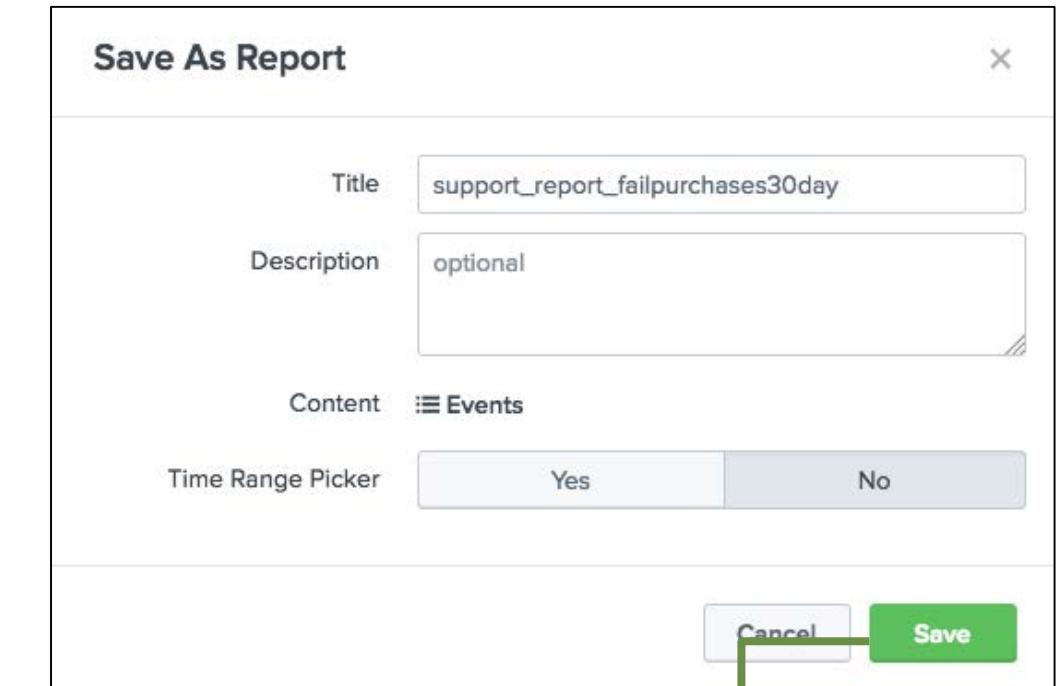
- A Give the report a meaningful title (required)
- B Specify a description (optional)
- C Select whether to include or not to include a time range picker
  - The report is saved with the time range that was selected when it was created
  - Adding a time range picker allows you to adjust the time range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



Generated for () (C) Splunk Inc, not for distribution

# Creating a Report from a 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

Generated for () (C) Splunk Inc, not for distribution

# Running Reports

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

The screenshot shows the Splunk web interface. On the left, there's a sidebar with tabs for Search, Datasets, Reports (which is selected), and Alerts. Below the tabs, there's a section for Reports with a brief description and a list of 7 reports. One report, 'support\_report\_failpurchases30day', is highlighted. The main area displays the report results for 'support\_report\_failpurchases30day'. The title bar says 'support\_report\_failpurchases30day' with options to Edit, More Info, and Add to Dashboard. It shows a summary of 953 events from 12/9/17 to 1/8/18. The results table has columns for i, Time, and Event. Two events are listed:

| i | Time                     | Event  |
|---|--------------------------|--|
| > | 1/8/18<br>9:36:36.000 AM | 123.196.113.11 - - [08/Jan/2018:09:36:36] "POST /cart.do?action=purchase&itemId=EST-14&JSESSIONID=SD1SL8FF6ADFF4958 HTTP 1.1" 503 2873 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-14&categoryId=SIMULATION&productId=SC-MG-G10" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 131<br>host = www2   source = /opt/log/www2/access.log   sourcetype = access_combined |
| > | 1/8/18<br>8:43:19.000 AM | 94.230.166.185 - - [08/Jan/2018:08:43:19] "GET /cart.do?action=purchase&itemId=EST-15&JSESSIONID=SD1SL8FF9ADFF4958 HTTP 1.1" 400 2106 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-15" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 818<br>host = www3   source = /opt/log/www3/access.log   sourcetype = access_combined   |

Below the table, there are buttons for Open in Search, Edit, None, nobody, search, App, and Private.

Generated for () (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 the Splunk interface for editing a report named "support\_report\_failpurchases30day". The report displays 953 events from December 9, 2017, to January 8, 2018. The search command is:

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

The interface includes tabs for Events (953), Patterns, Statistics, and Visualization. A context menu is open on the right, with "Open in Search" highlighted. Other options in the menu include:

- Edit Description
- Edit Permissions
- Edit Schedule
- Edit Acceleration
- Clone
- Embed
- Delete

The bottom of the interface shows a footer with the text "Generated for () (C) Splunk Inc, not for distribution".

# Creating Tables and Visualizations

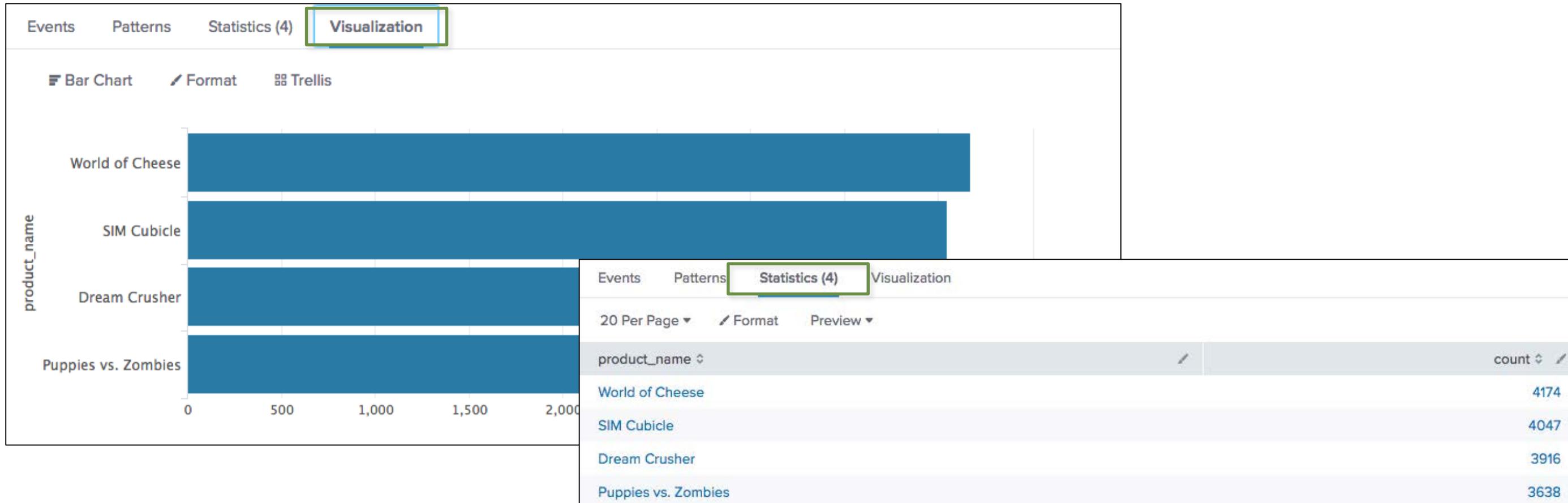
---

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

1. Select a field from the fields sidebar and choose a report to run
2. Use the Pivot interface
  - Start with a dataset  
*or*
  - Start with Instant Pivot
  - See Module 11 in this presentation for more information about Pivot
3. Use the Splunk search language transforming commands in the Search bar

# Viewing Tables and Visualizations

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



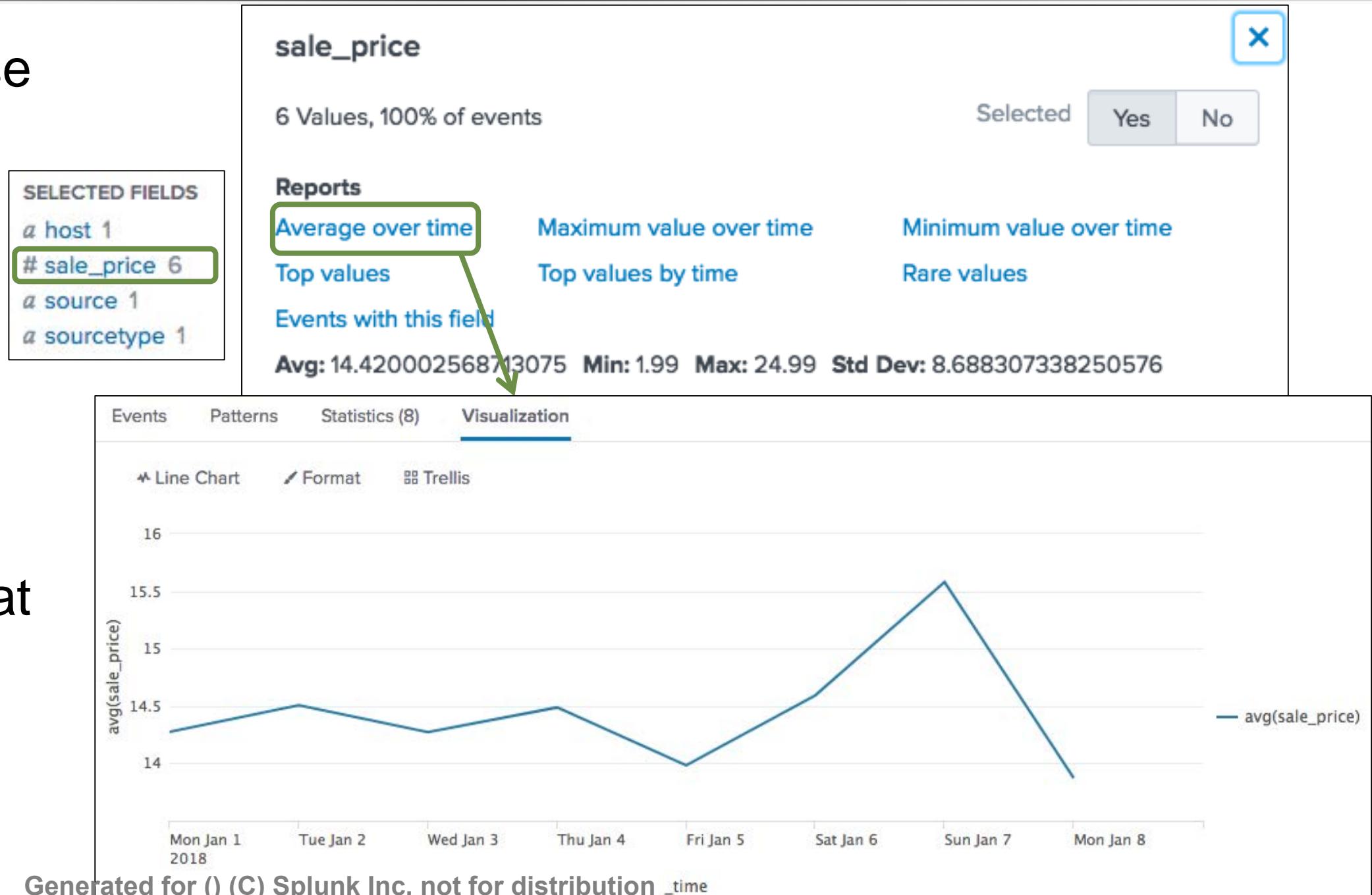
Generated for () (C) Splunk Inc, not for distribution

# Creating Reports From the Field Window

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

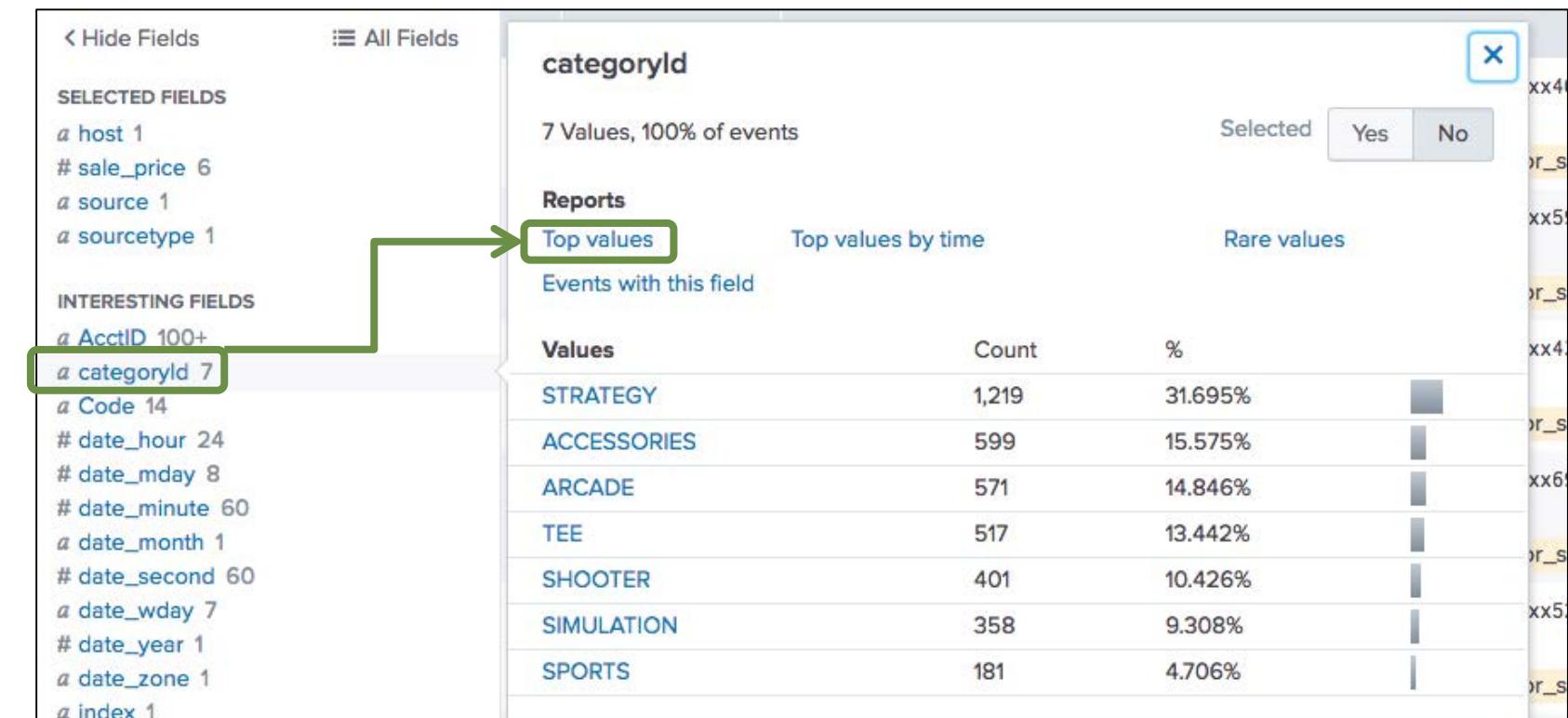
- This example generates a report that shows the average over time

– This is known as a **timechart**



# Creating a Top Values Report

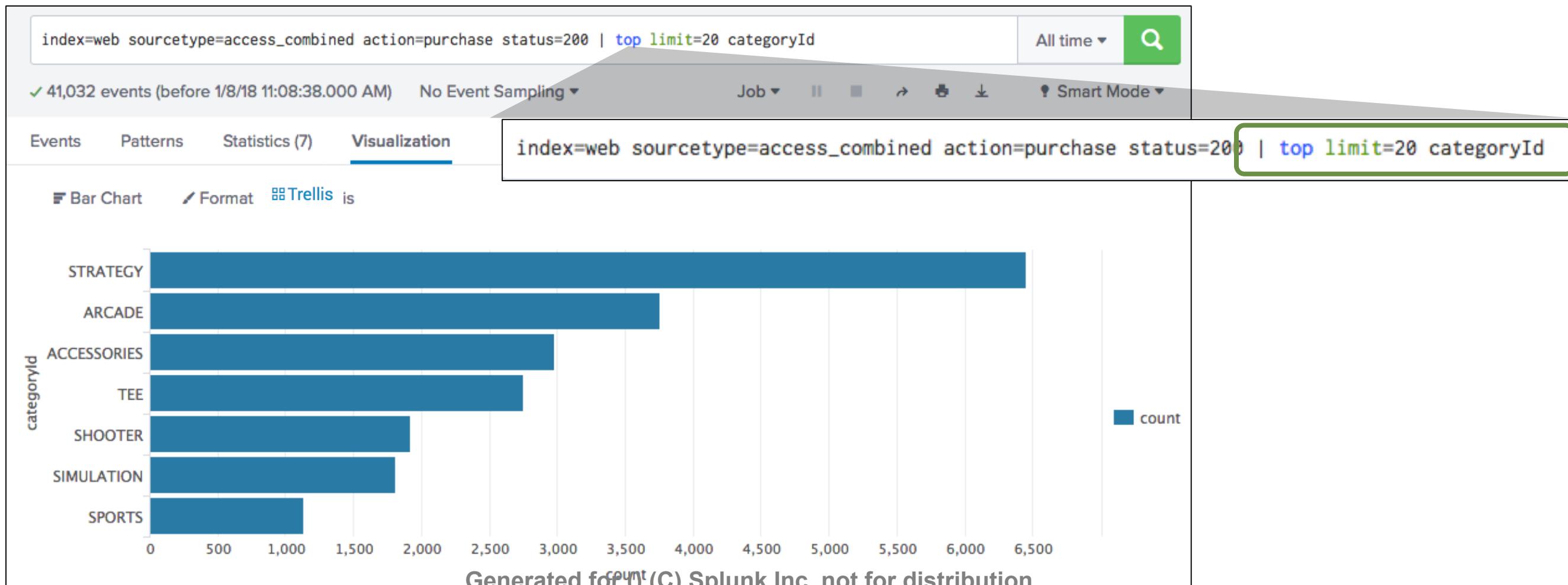
- For alphanumeric character fields, there are only 3 available reports
- In this example, you want a report that shows the top **categories** purchased
  1. Run basic search: sourcetype=access\_combined status=200 action=purchase
  2. Click the **categoryId** field
  3. Click **Top values**



Generated for () (C) Splunk Inc, not for distribution

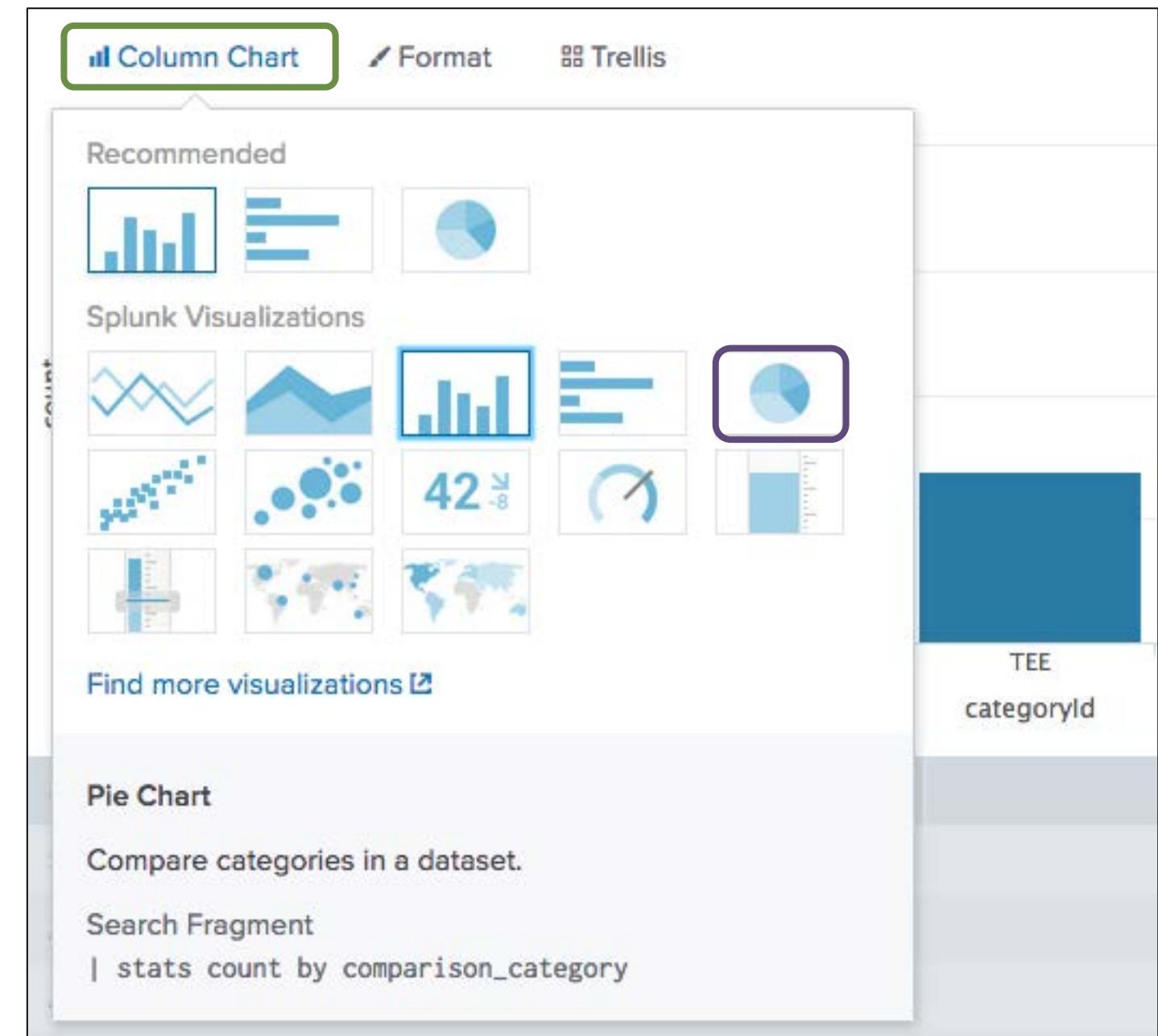
# Creating a Top Values Report (cont.)

4. The top command with limit=20 is added to the search string
5. A bar chart is returned on the Visualizations tab, displaying the top categories purchased



# Changing the Visualization

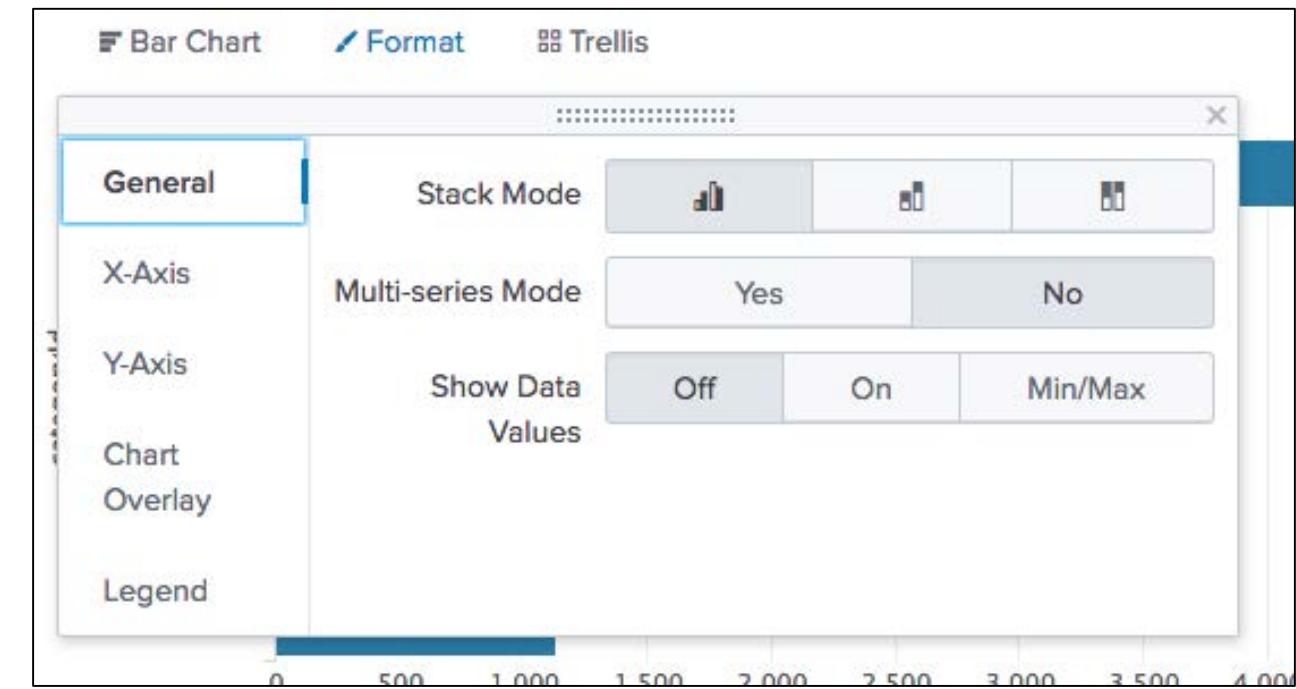
- Select a visualization from the visualization type dropdown menu
- In this example, the column chart is changed to a pie chart



Generated for () (C) Splunk Inc, not for distribution

# Changing the Visualization Format

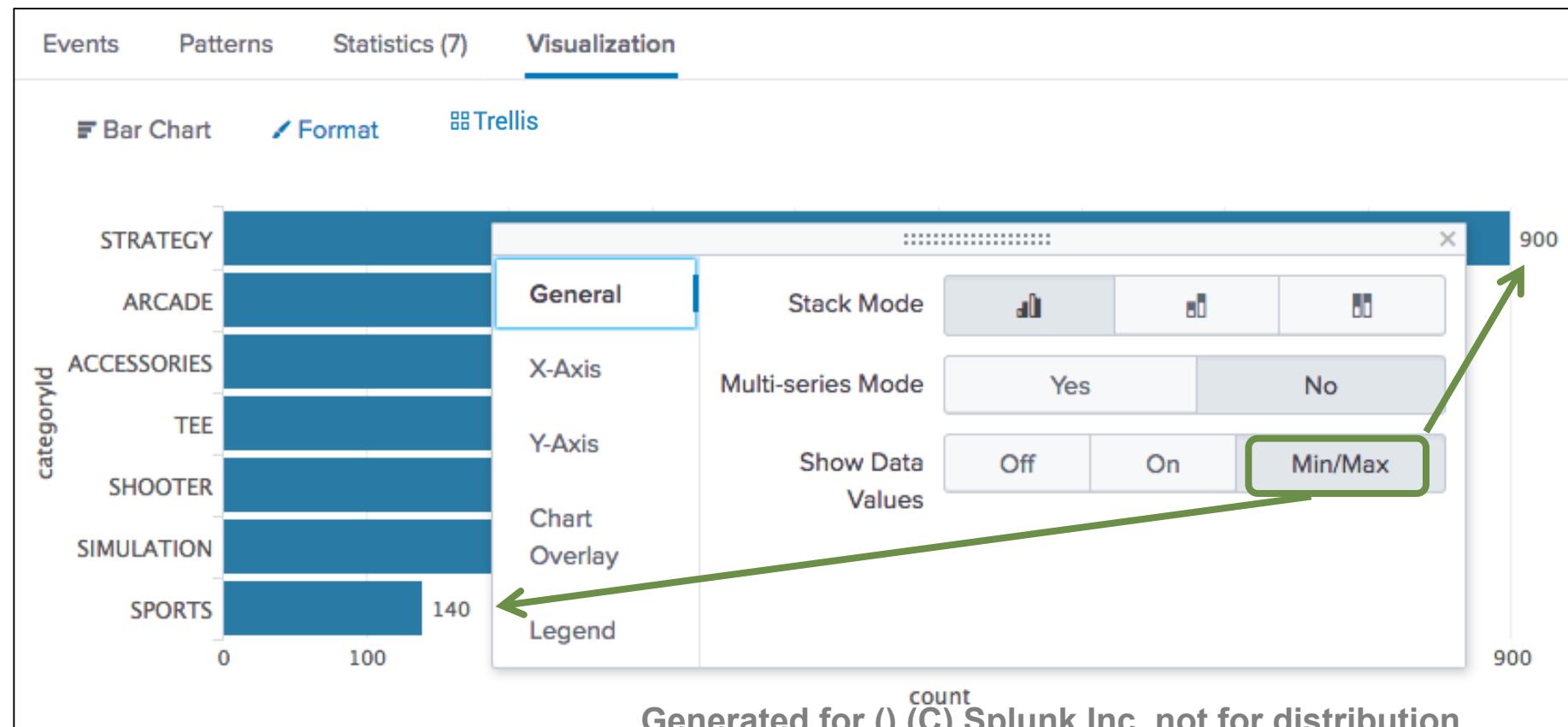
- The **Format** menu allows you to change formatting options
- For example, for bar and column charts:
  - The **General** tab allows you to change Stack and Multi-series modes
  - The **X-Axis** and **Y-Axis** tabs allow you to change the axis labels and orientation
  - **Chart Overlay** allows you to add context to the chart by overlaying other field values



- The **Legend** tab allows you to position the visualization legend as desired
- **Stack Mode** allows you to stack colors to improve column chart readability when several colors are involved

# Changing the Visualization 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



## Note

When you make a change to the visualization settings – such as Min/Max – the visualization updates immediately.

## Note

Learn more about modes and axes in the *Splunk Fundamentals 2* course. These modes require more sophisticated searches.

# Viewing Results as a Table

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

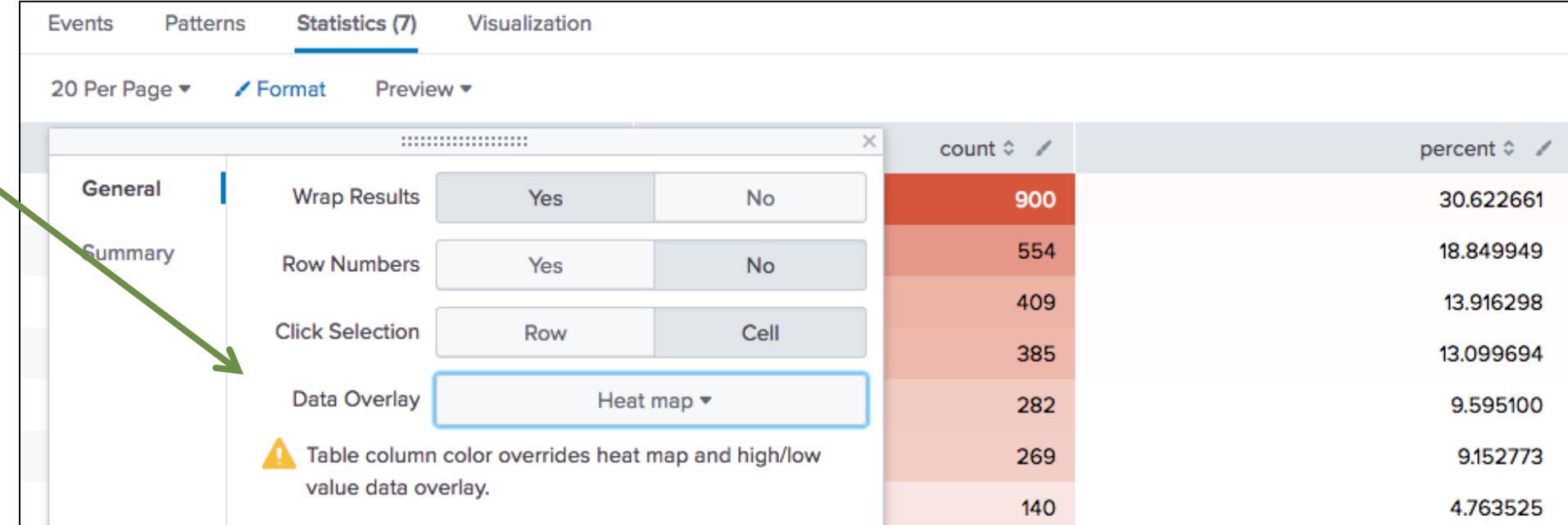
The screenshot shows the Splunk interface with the Statistics tab selected. The table lists categories and their counts and percentages:

| categoryId  | count | percent   |
|-------------|-------|-----------|
| STRATEGY    | 900   | 30.622661 |
| ARCADE      | 554   | 18.849949 |
| ACCESSORIES | 409   | 13.916298 |
| TEE         | 385   | 13.099694 |
| SHOOTER     | 282   | 9.595100  |
| SIMULATION  | 269   | 9.152773  |
| SPORTS      | 140   | 4.763525  |

Generated for () (C) Splunk Inc, not for distribution

# Using the Data Overlay Format

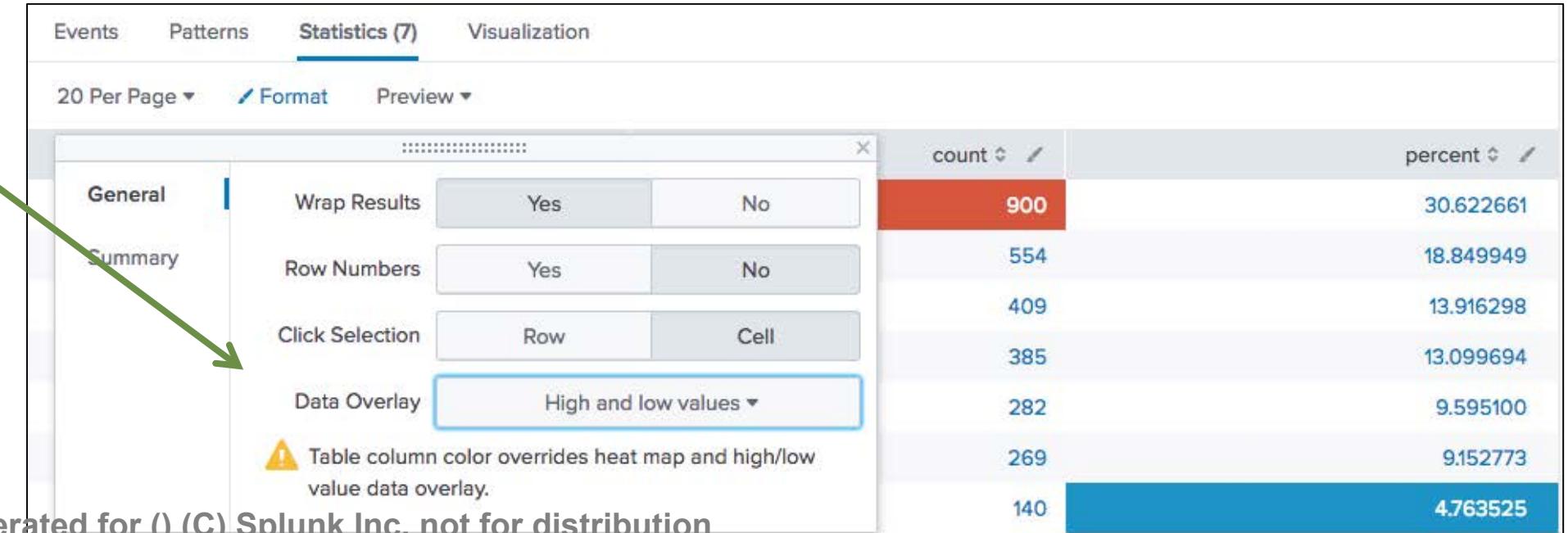
- Heat map highlights outstanding values



The screenshot shows the Splunk Statistics interface with the 'Heat map' option selected under 'Data Overlay'. A green arrow points from the text 'Heat map highlights outstanding values' to this selection. The interface includes tabs for Events, Patterns, Statistics (7), and Visualization, with 'Statistics' being the active tab. It also shows options for 'Wrap Results', 'Row Numbers', 'Click Selection', and a warning about table column colors overriding the overlay.

|  | count | percent   |
|--|-------|-----------|
|  | 900   | 30.622661 |
|  | 554   | 18.849949 |
|  | 409   | 13.916298 |
|  | 385   | 13.099694 |
|  | 282   | 9.595100  |
|  | 269   | 9.152773  |
|  | 140   | 4.763525  |

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



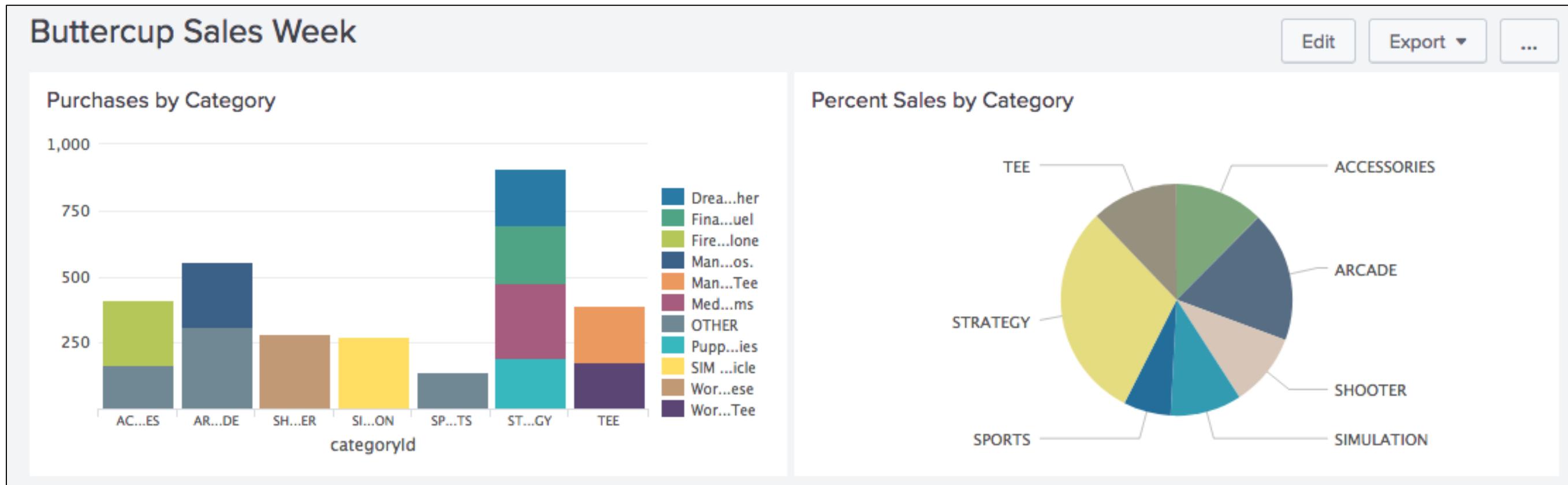
The screenshot shows the Splunk Statistics interface with the 'High and low values' option selected under 'Data Overlay'. A green arrow points from the text 'High and low values highlights max and min of non zero values' to this selection. The interface is identical to the first screenshot, with the 'Heat map' option previously selected.

|  | count | percent   |
|--|-------|-----------|
|  | 900   | 30.622661 |
|  | 554   | 18.849949 |
|  | 409   | 13.916298 |
|  | 385   | 13.099694 |
|  | 282   | 9.595100  |
|  | 269   | 9.152773  |
|  | 140   | 4.763525  |

Generated for () (C) Splunk Inc, not for distribution

# What Is a Dashboard?

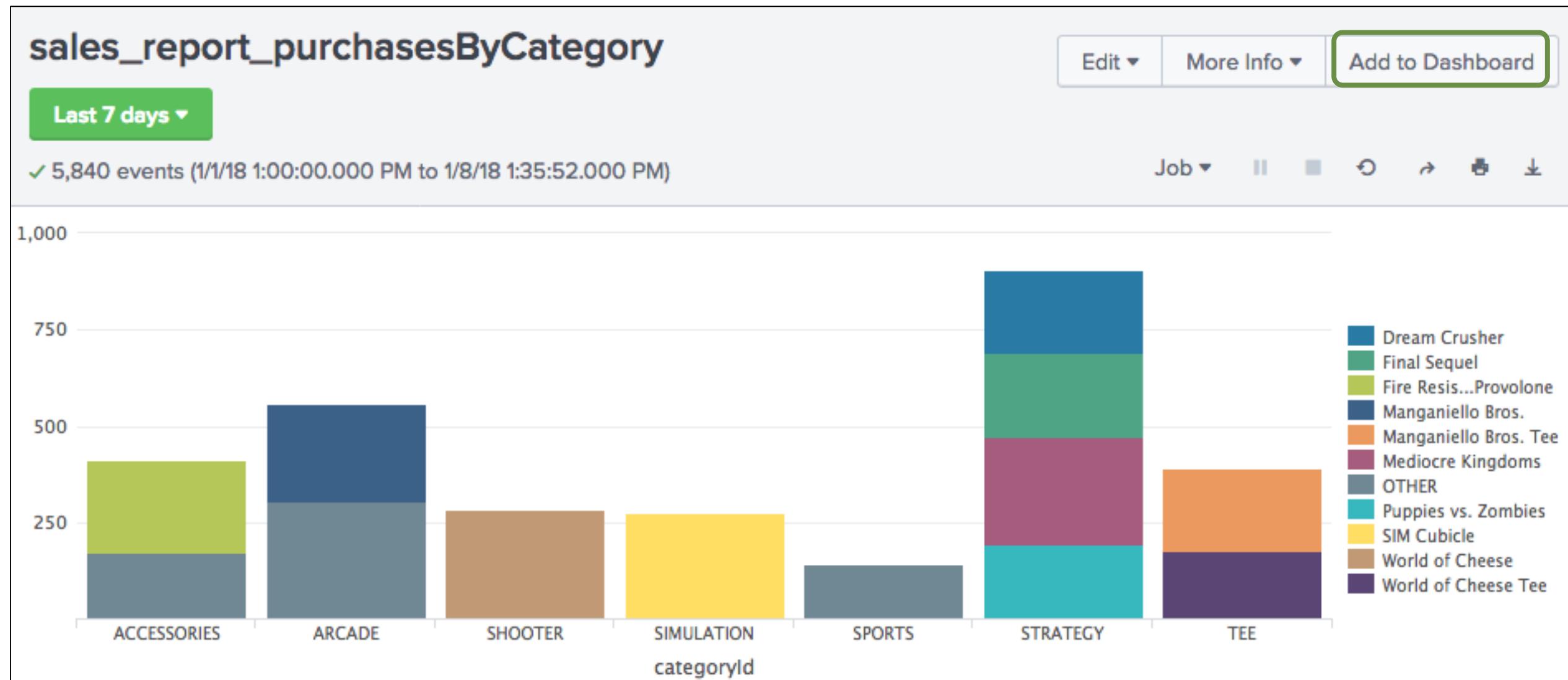
- A dashboard consists of one or more panels displaying data visually in a useful way – such as events, tables, or charts
- A report can be used to create a panel on a dashboard



Generated for () (C) Splunk Inc, not for distribution

# Adding a Report to a Dashboard

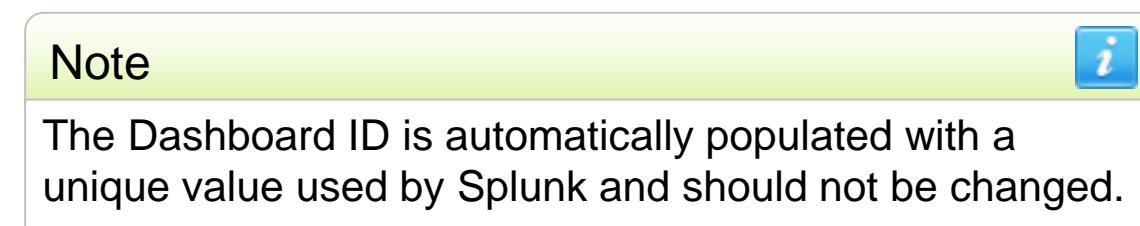
In the report, click Add to Dashboard to begin



Generated for () (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 Panel Content, click Column Chart to display the visualization in the dashboard



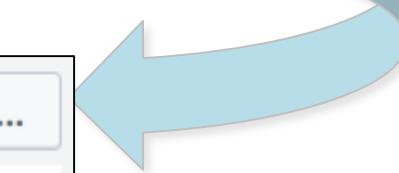
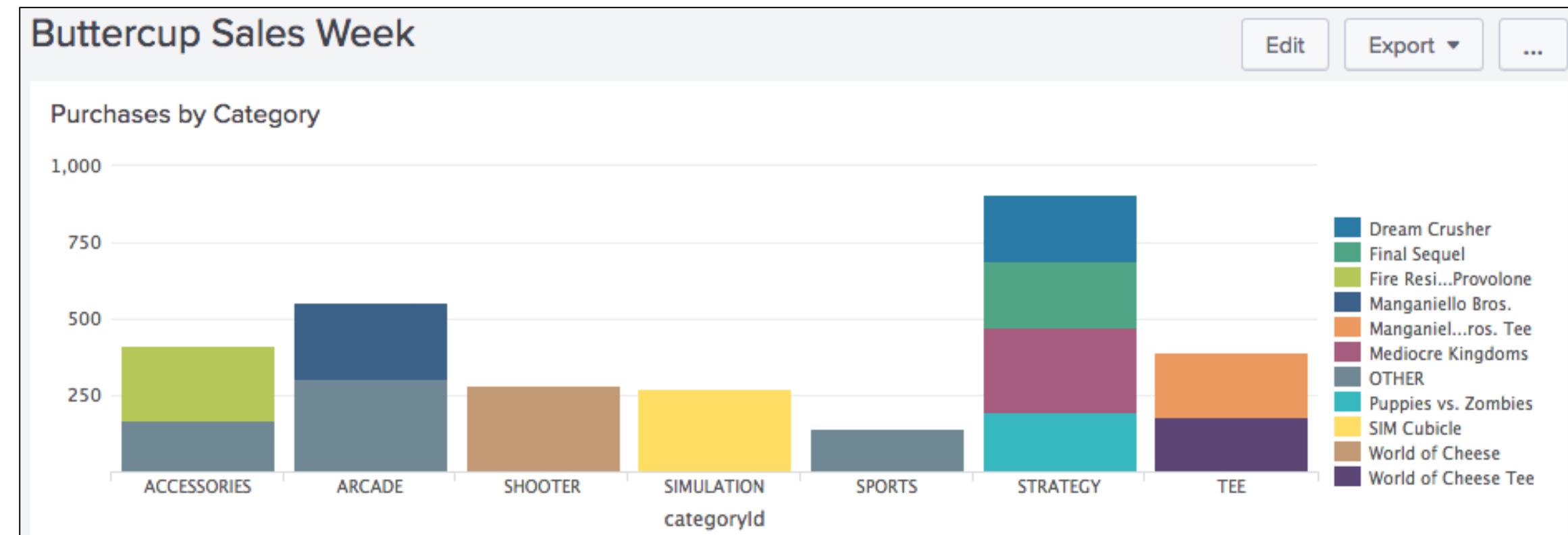
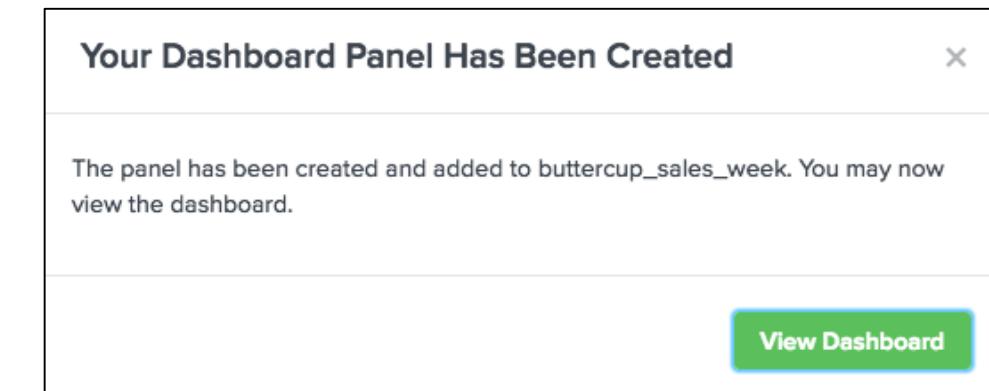
Save As Dashboard Panel

|   |   |  |   |
|---|---|--|---|
| 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                              | <input type="text"/> Inline Search          | <input checked="" type="radio"/> Report            | D |
| Drilldown ?                                   | No action                                   |  |   |
| Panel Content                                 | <input checked="" type="radio"/> Statistics | <input type="radio"/> Column Chart                 | E |
| <button>Cancel</button> <button>Save</button> |   |  |   |

Generated for () (C) Splunk Inc, not for distribution

# 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



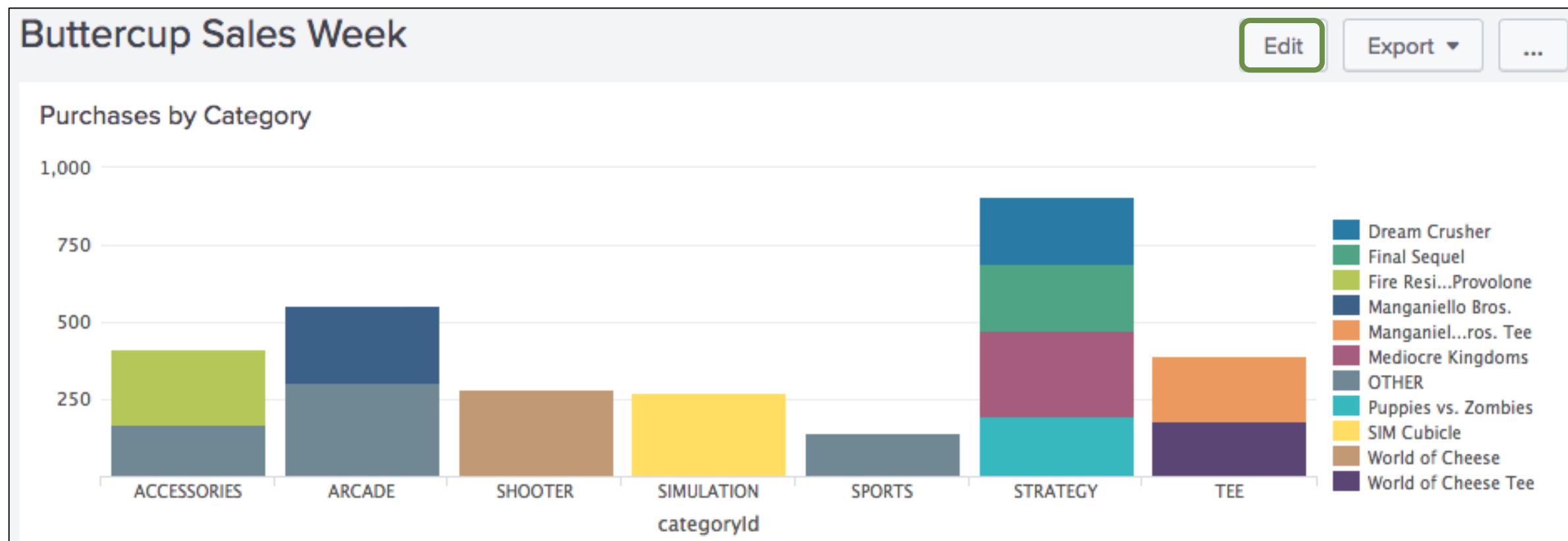
# Why Create Panels from Reports?

---

- 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 affects every dashboard panel that utilizes that report

# Editing Panels

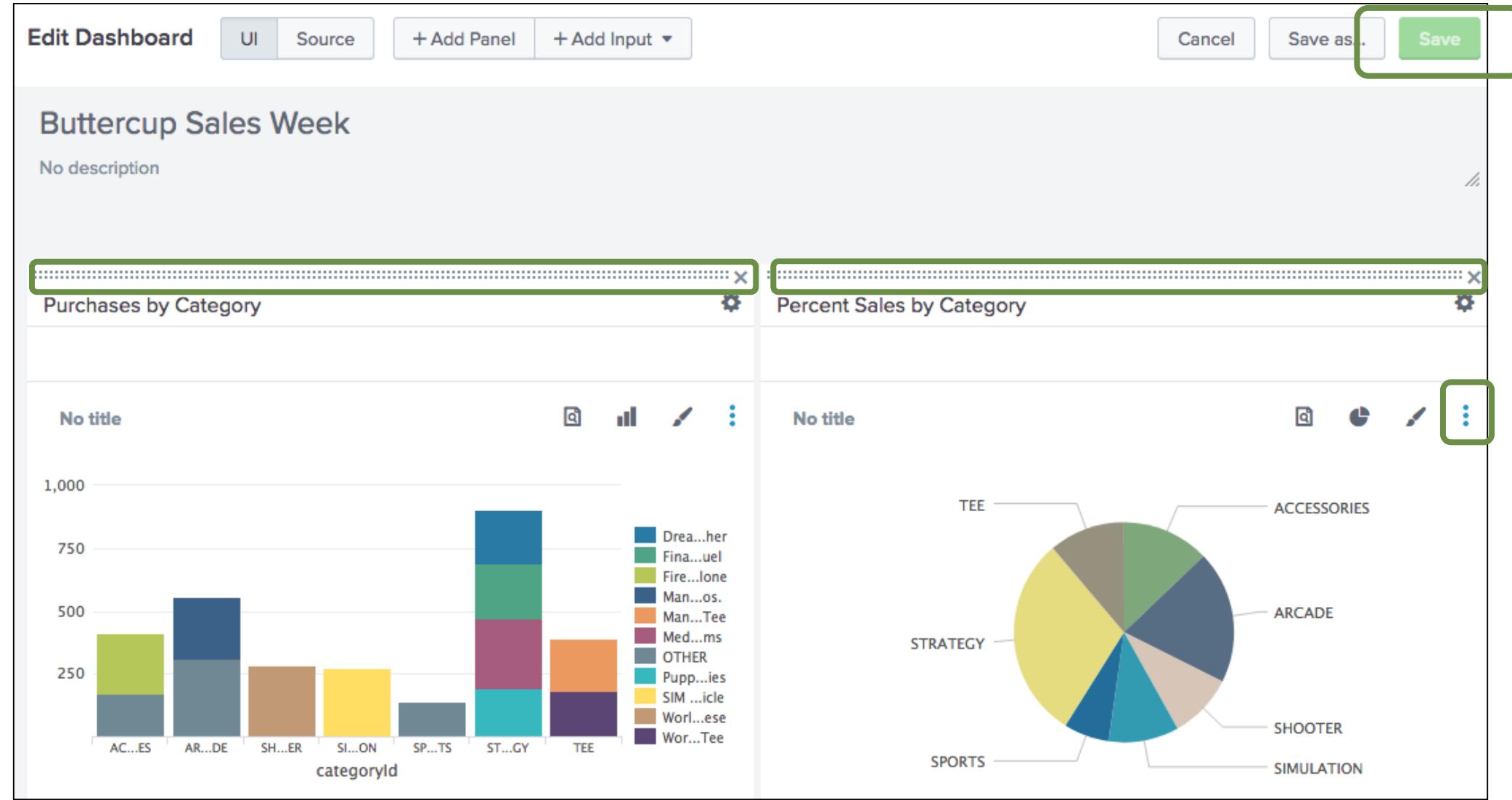
- After saving the panel, a window appears from which you can view the updated dashboard
- Click Edit to customize the dashboard



Generated for () (C) Splunk Inc, not for distribution

# Editing Panel Layout

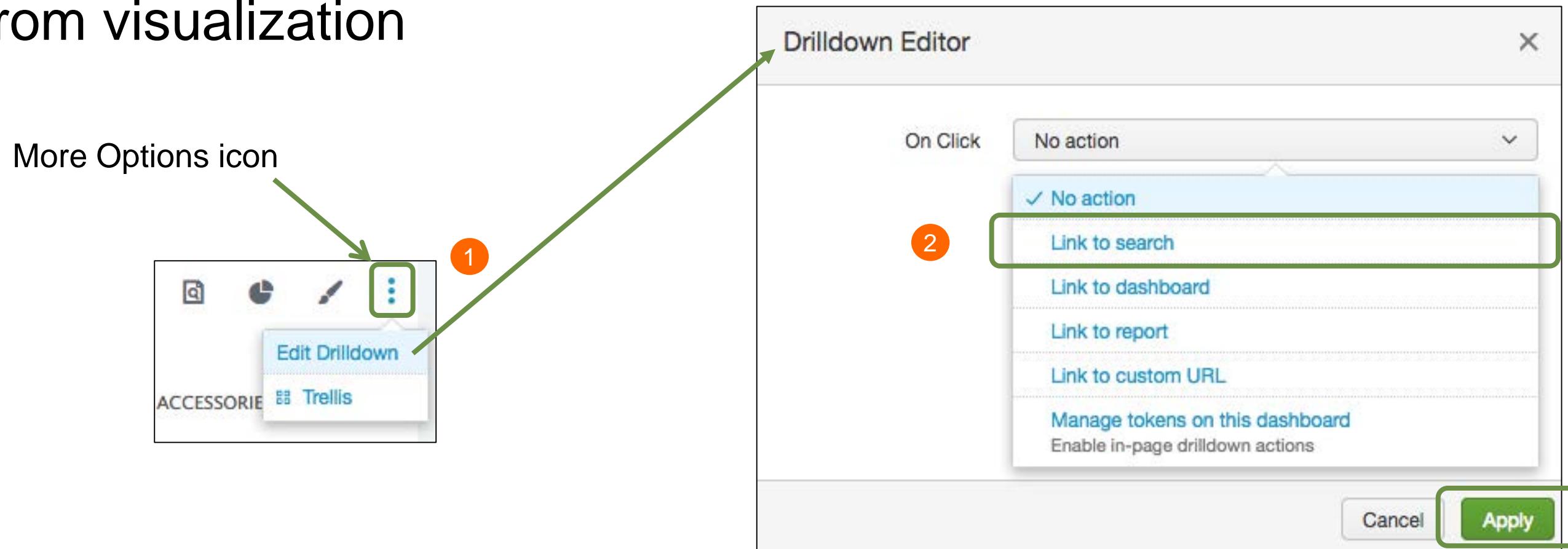
Click on the dotted bar on a panel to drag the panel to a new location



More Options icon  
(discussed on next slide)

# Edit Panel Drilldown Options

1. In Edit Dashboard mode, click the More Options icon on any panel and select Edit Drilldown
2. In Drilldown Editor, select Link to search to access search directly from visualization



Generated for () (C) Splunk Inc, not for distribution

# Drilldown from Visualization to Search

Once drilldown option is set, click an object in a chart or table to see its underlying events in Search view

New Search

index=web sourcetype=access\_combined action=purchase status=200 categoryId=STRATEGY

✓ 110 events (1/7/18 2:00:00.000 PM to 1/8/18 2:43:25.000 PM) No Event Sampling ▾

Save As ▾ Close Date time range ▾

Job ▾ II ■ ▾ Smart Mode ▾

Events (110) Patterns Statistics Visualization

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

List ▾ Format 20 Per Page ▾

< Prev 1 2

Time Event

1/8/18 2:39:31.000 PM 192.162.19.179 -- [08/Jan/2018:14:39:31] "POST /cart.do?act...  
IONID=SD0SL5FF5ADFF4953 HTTP/1.1" 200 3567 "http://www.buttercupg...  
dtocart&itemId=EST-7&categoryId=STRATEGY&productId=FS-SG-C03"  
ntel Mac OS X 10\_6\_3; en-US) AppleWebKit/533.4 (KHTML, like  
/533.4" 650  
host = www3 | source = /opt/log/www3/access.log | sourcetype = access\_log

SELECTED FIELDS  
host 3  
source 3  
sourcetype 1

INTERESTING FIELDS  
action 1  
# bytes 100+  
categoryId 1

Generated for () (C) Splunk Inc, not for distribution

categoryId: STRATEGY  
count: 110  
count%: 30.055%

# Clone a Dashboard

1. Click the ellipsis menu (...) and select **Clone**
2. Change the **Title** as desired and click **Clone Dashboard**

Buttercup Sales Week

Purchases by Category

| categoryid | Purchases |
|------------|-----------|
| AC...ES    | 400       |
| AR...DE    | 300       |
| SH...ER    | 200       |
| SI...ON    | 200       |
| SP...TS    | 100       |
| ST...GY    | 400       |
| TEE        | 300       |

Percent Sales by Category

| Category  | Percentage |
|-----------|------------|
| TEE       | 30%        |
| STRATEGY  | 30%        |
| SPORTS    | 20%        |
| OTHER     | 10%        |
| Wor...Tee | 5%         |
| Wor...ese | 5%         |

Edit Export ...

... (highlighted with a green box)

Edit Permissions

Clone (highlighted with a green box)

Set as Home Dashboard

Delete

Clone

Title: Buttercup Sales Week Clone

ID: buttercup\_sales\_week\_clone

New Description: optional

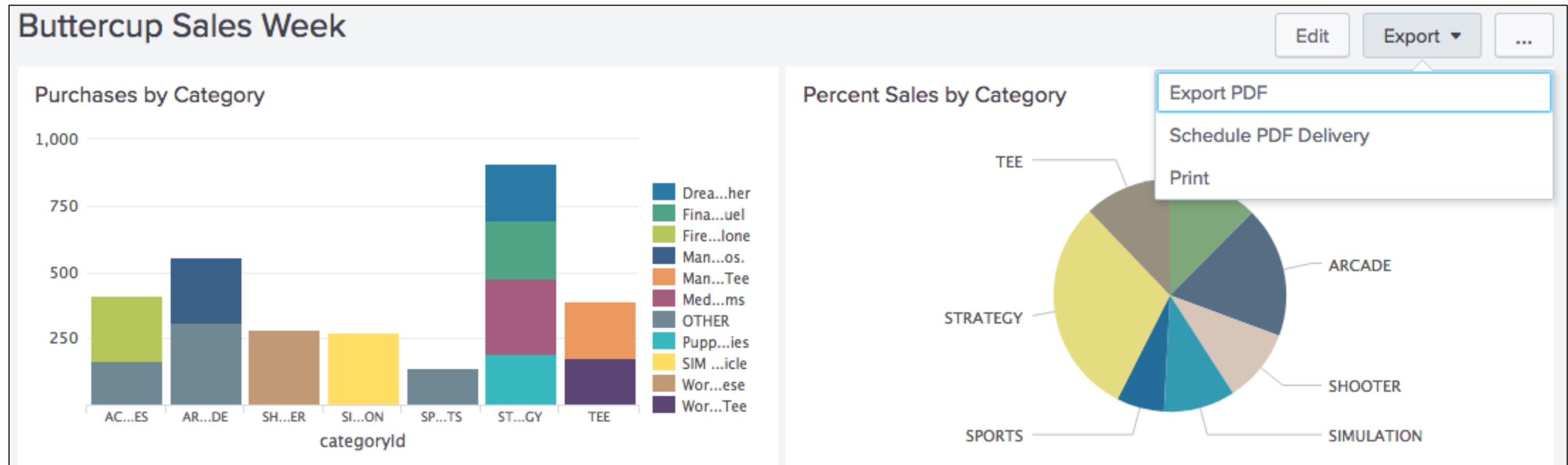
Cancel

Clone Dashboard (highlighted with a green box)

Generated for () (C) Splunk Inc, not for distribution

# Export a Dashboard

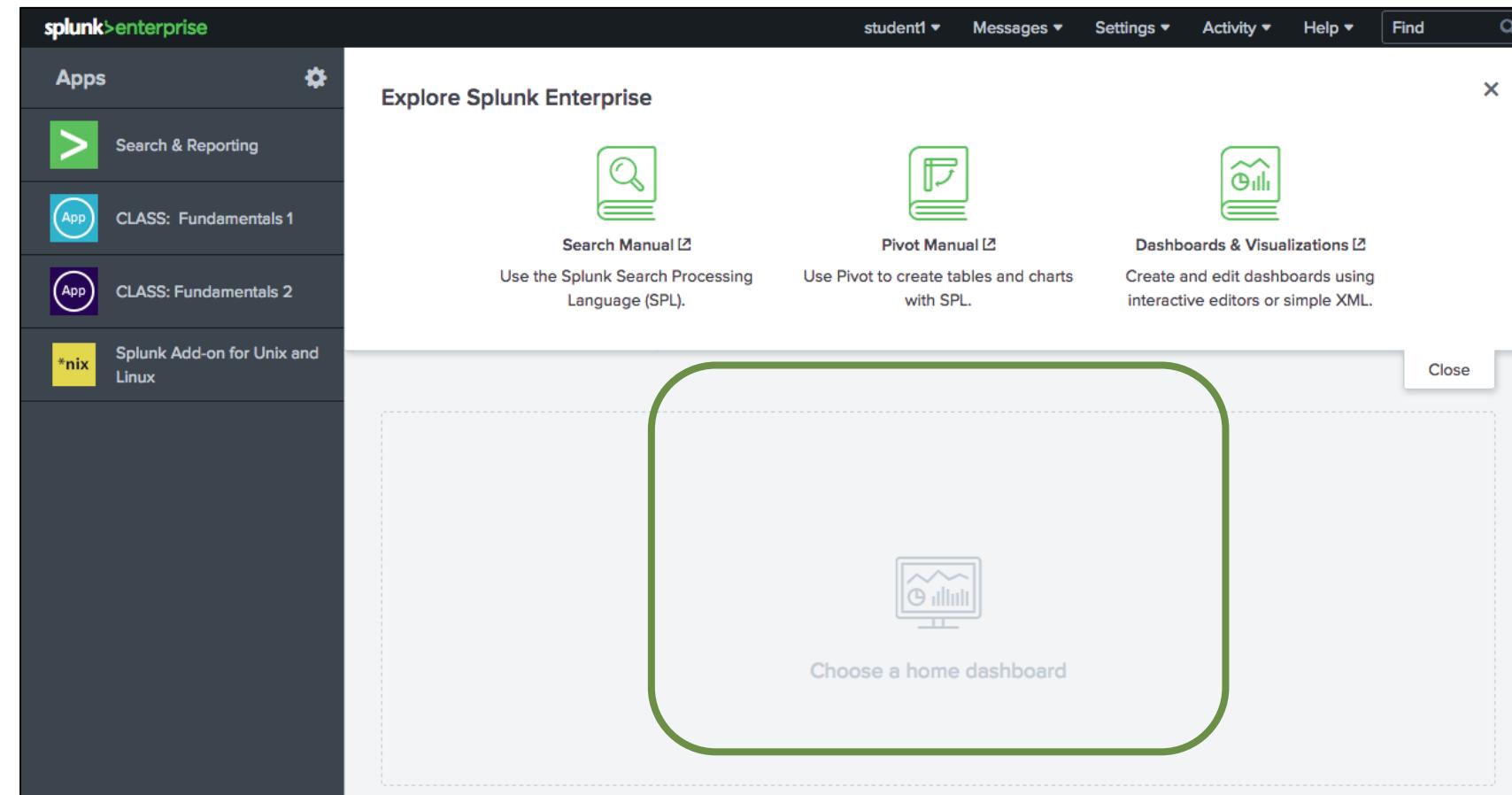
Dashboards can be exported as PDF or printed



Generated for () (C) Splunk Inc, not for distribution

# Set the Default Dashboard

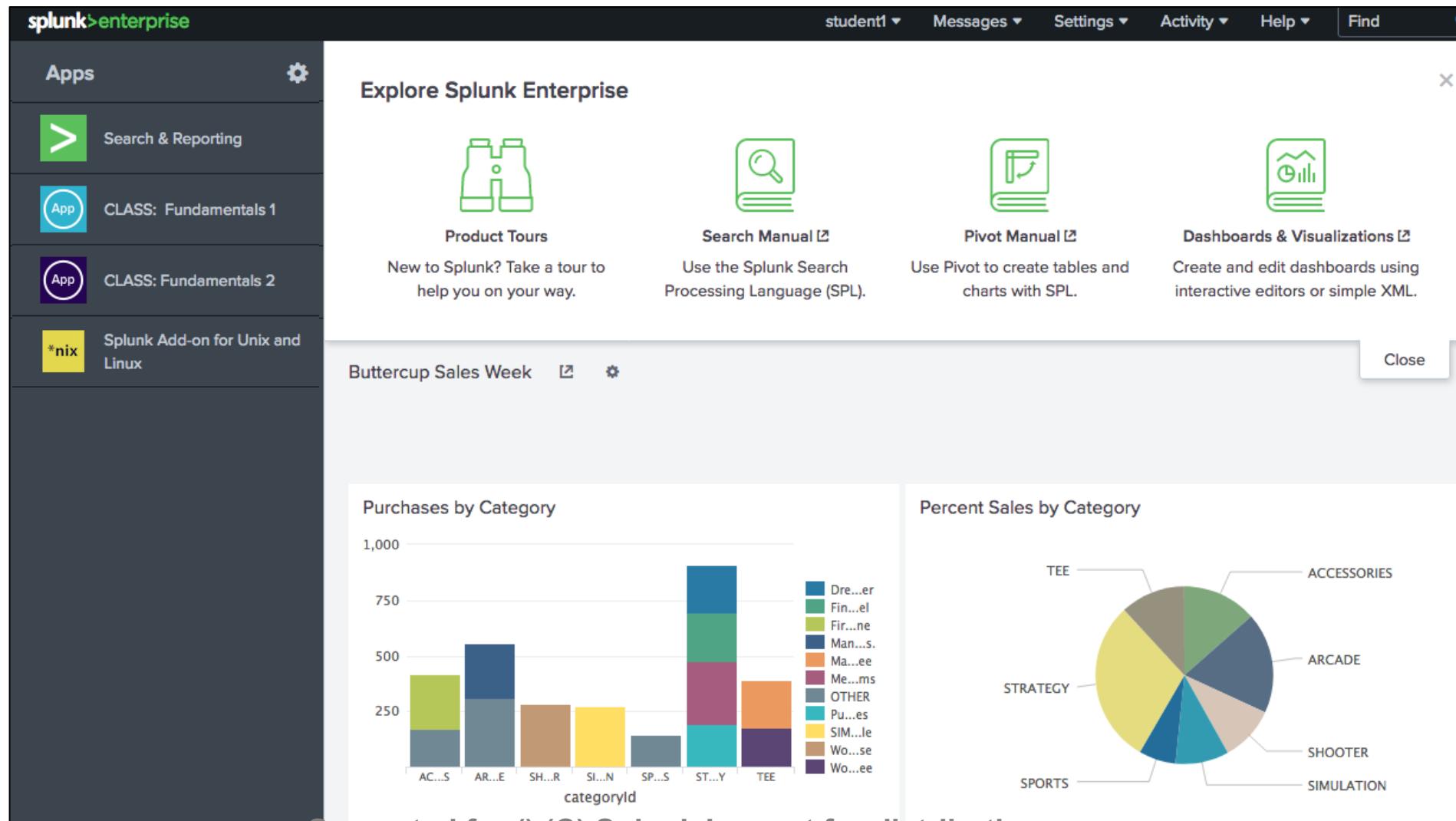
- Set a dashboard to appear by default in the bottom panel of your home view
- From the Home app, click **Choose a home dashboard**



Generated for () (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:



# Module 11

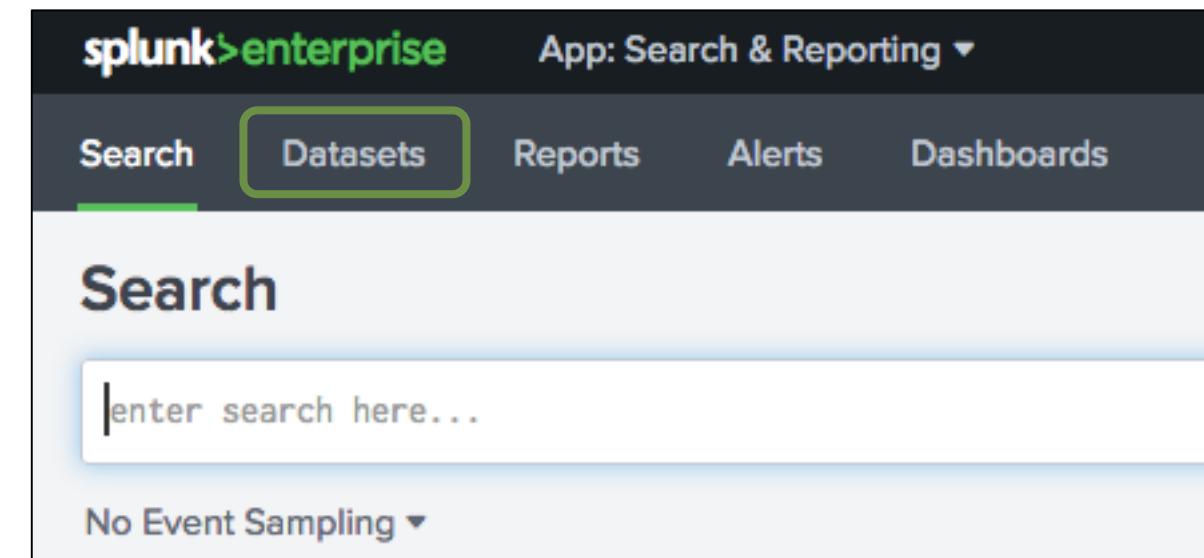
# Pivot & Datasets

Generated for () (C) Splunk Inc, not for distribution

# Selecting a Dataset

1. From the Search & Reporting app, select the **Datasets** tab
  - 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**



|   |            |   |                       |
|---|------------|---|-----------------------|
| > Buttercup Games Online Sales > Web Requests                   | data model | ⚡ | Explore ▾             |
| > Buttercup Games Online Sales > Web Requests > Failed Reqe...  | data model | ⚡ | Explore ▾             |
| > Buttercup Games Online Sales > Web Requests > Failed Reqe...  | data model | ⚡ | Explore ▾             |
| > Buttercup Games Online Sales > Web Requests > Failed Reqe...  | data model | ⚡ | Explore ▾             |
| > Buttercup Games Online Sales > Web Requests > Failed Reqe...  | 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  |
| > Buttercup Games Online Sales > Web Requests > Successful R... | data model | ⚡ | Investigate in Search |

Generated for () (C) Splunk Inc, not for distribution

# Opening 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

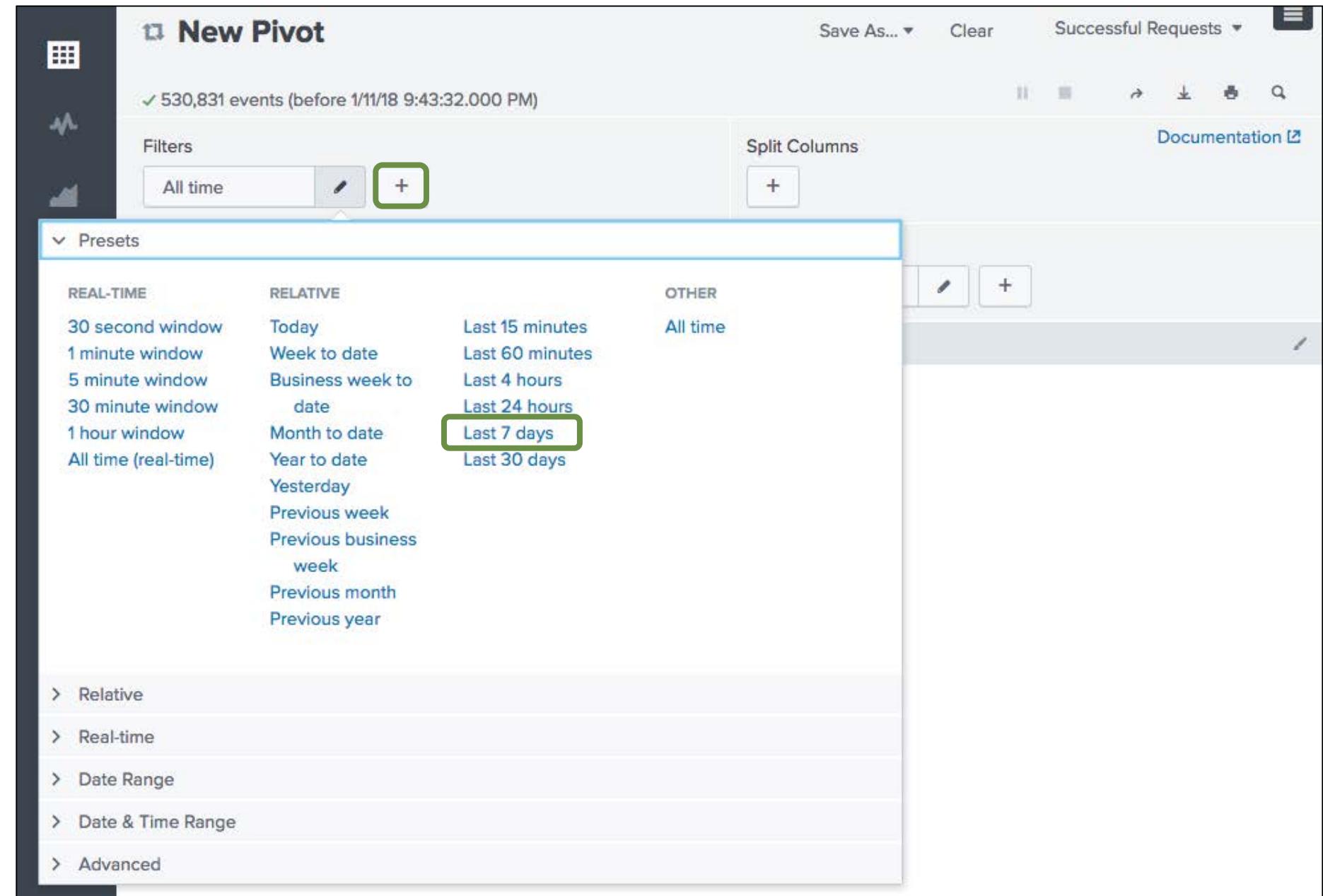
The screenshot shows the Splunk Pivot interface with the following details:

- Title:** New Pivot
- Event Count:** 530,831 events (before 1/11/18 9:43:32.000 PM)
- Filters:** All time
- Split Rows:** +
- Column Values:** Count of Suc... (highlighted with a green box)
- Count of Successful Requests:** 530831 (highlighted with a green box)
- Buttons:** Save As..., Clear, Documentation, Split Columns, +

Generated for () (C) Splunk Inc, not for distribution

# Selecting a Time Range

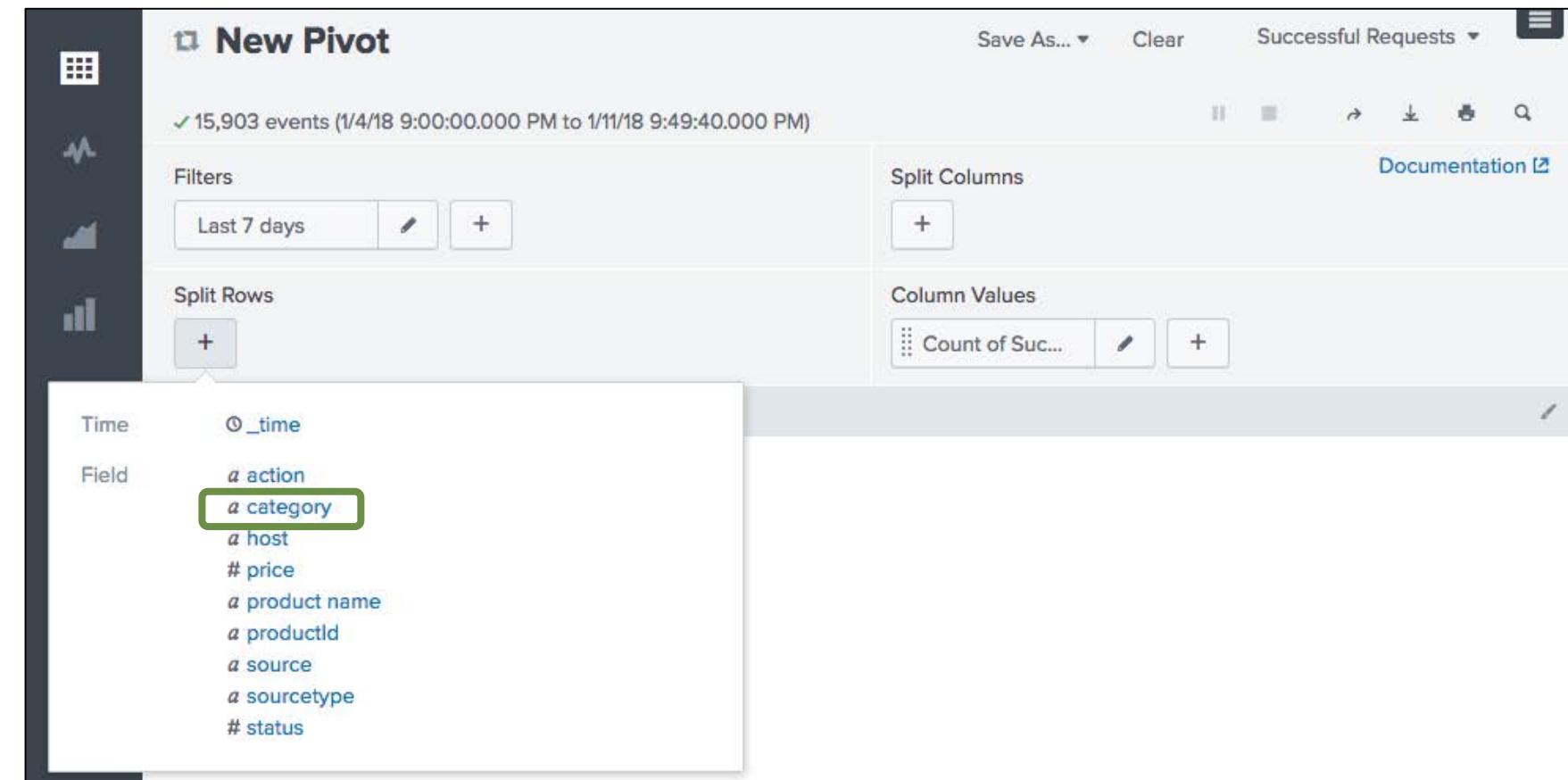
- The default is All time
- Click the pencil icon to select the desired time range
- The pivot runs immediately upon selecting the new time range



Generated for () (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 lists:
  - Each game category on a separate row
  - A count of successful requests for each game category

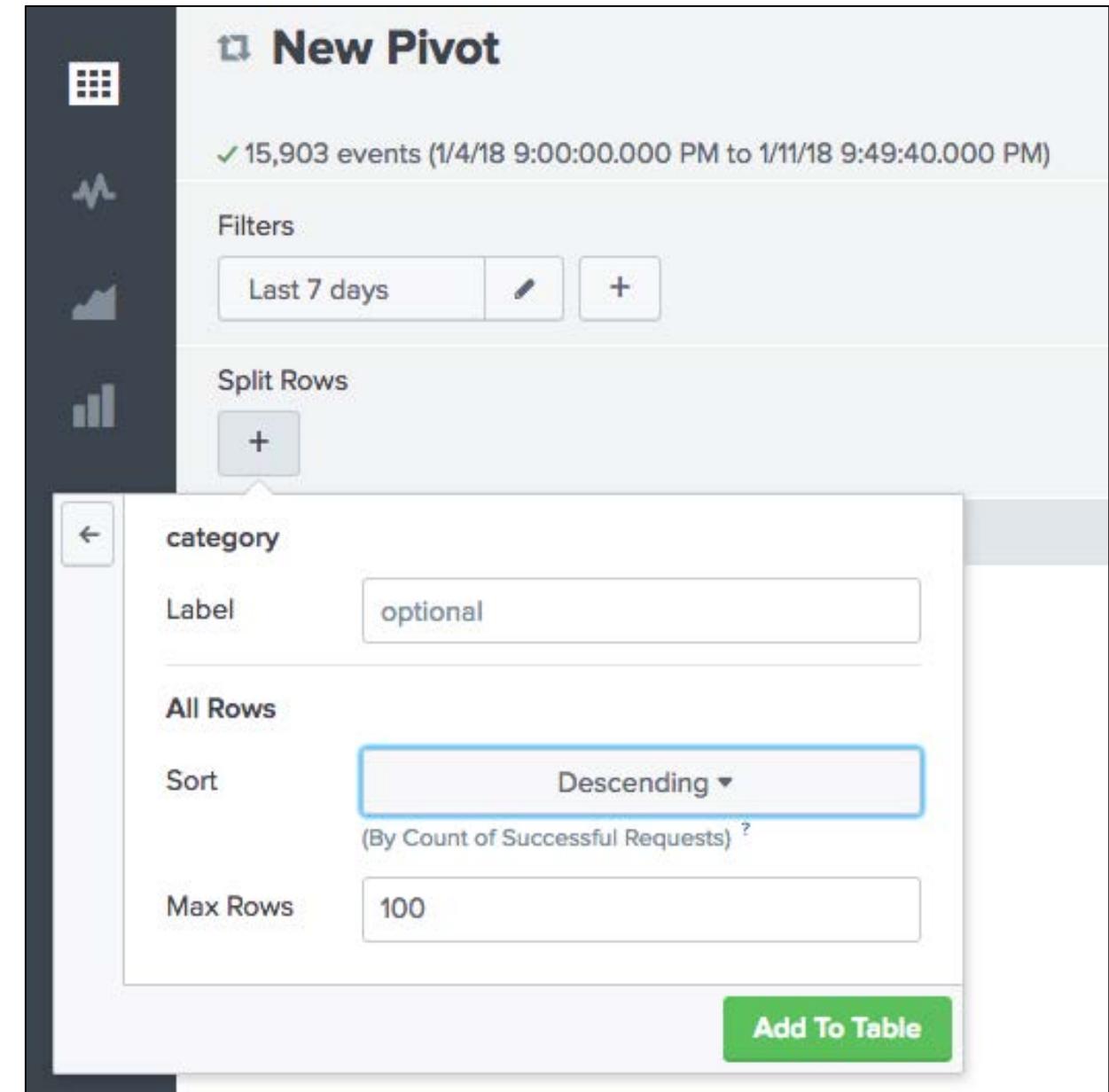


The screenshot shows the Splunk Pivot interface with a search titled "New Pivot" for 15,903 events from January 4, 2018, to January 11, 2018. The interface includes filters for "Last 7 days", a "Split Columns" section, and a "Column Values" section with a "Count of Suc..." metric. A modal window is open over the interface, showing the "Split Rows" dropdown menu. The menu lists various fields: Time, `@_time`; Field, `a action`, `a category` (which is highlighted with a green border), `a host`, `# price`, `a product name`, `a productId`, `a source`, `a sourcetype`, and `# status`.

Generated for () (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



Generated for () (C) Splunk Inc, not for distribution

# Results

The screenshot shows a Splunk interface titled "New Pivot" with the following details:

- Filters:** Last 7 days.
- Split Rows:** category
- Column Values:** Count of Suc...

| category    | Count of Successful Requests |
|-------------|------------------------------|
| STRATEGY    | 4745                         |
| ARCADE      | 2986                         |
| ACCESSORIES | 2303                         |
| TEE         | 2111                         |
| SHOOTER     | 1495                         |
| SIMULATION  | 1389                         |
| SPORTS      | 874                          |

A yellow callout box labeled "categories" points to the "category" column in the pivot table. Another yellow callout box labeled "count by category" points to the "Count of Successful Requests" column header. A third yellow callout box at the bottom left points to the "Format" button in the footer. The footer also includes "20 per page" and "Generated for () (C) Splunk Inc, not for distribution".

To format the results, click here

Generated for () (C) Splunk Inc, not for distribution

20 per page ▾ Format

Save As... Clear Successful Requests Documentation

category

Count of Successful Requests

STRATEGY 4745

ARCADE 2986

ACCESSORIES 2303

TEE 2111

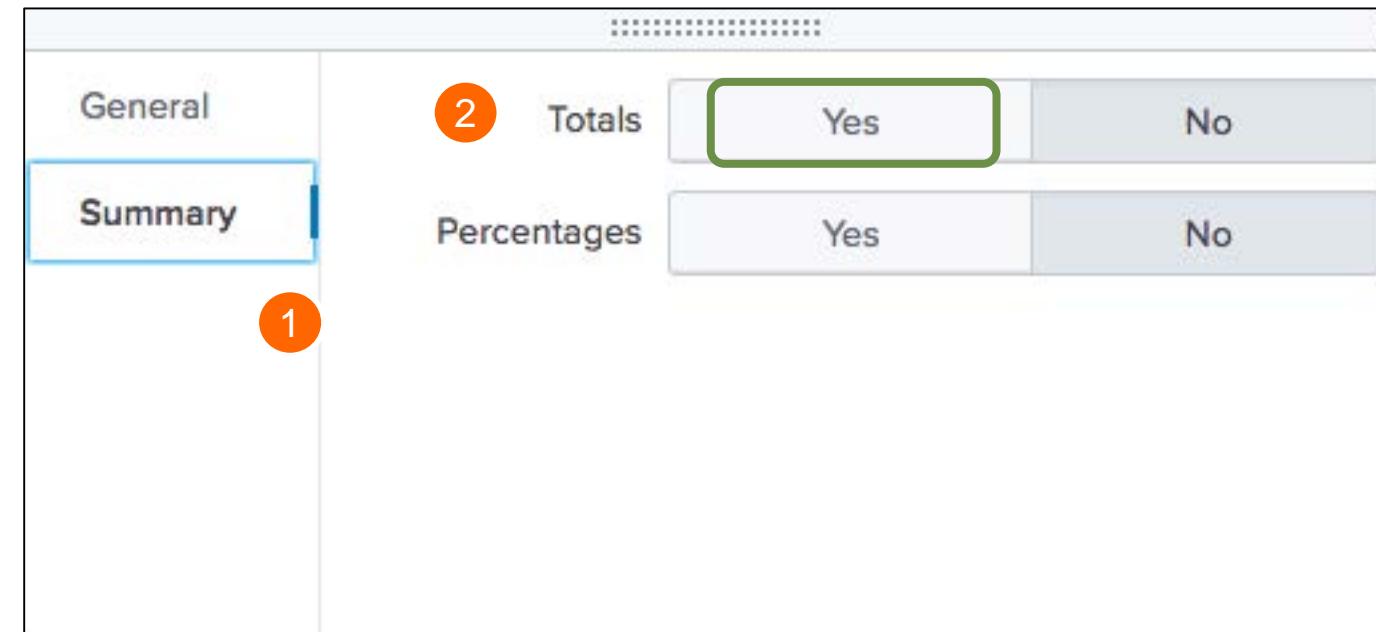
SHOOTER 1495

SIMULATION 1389

SPORTS 874

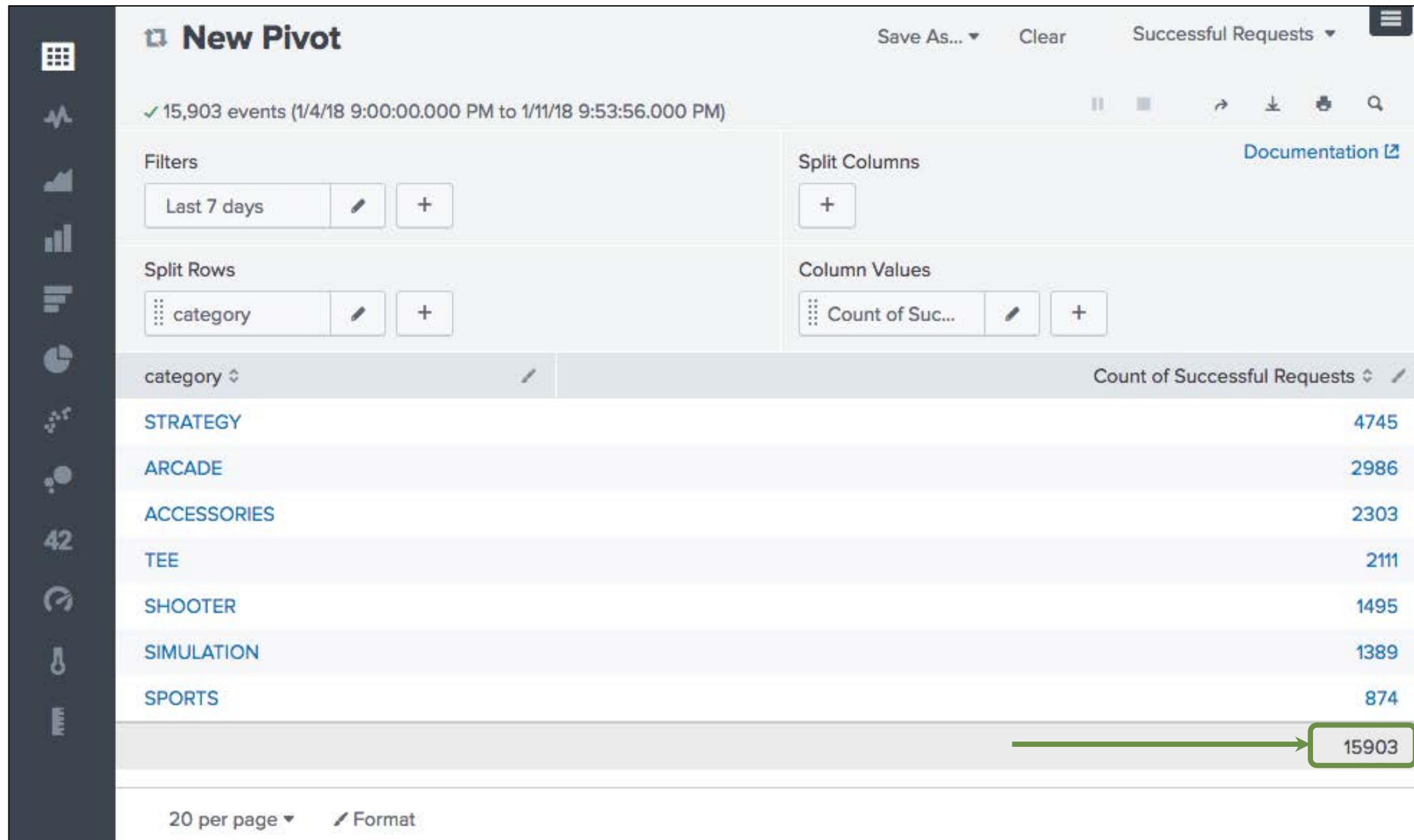
# Formatting the Results

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



Generated for () (C) Splunk Inc, not for distribution

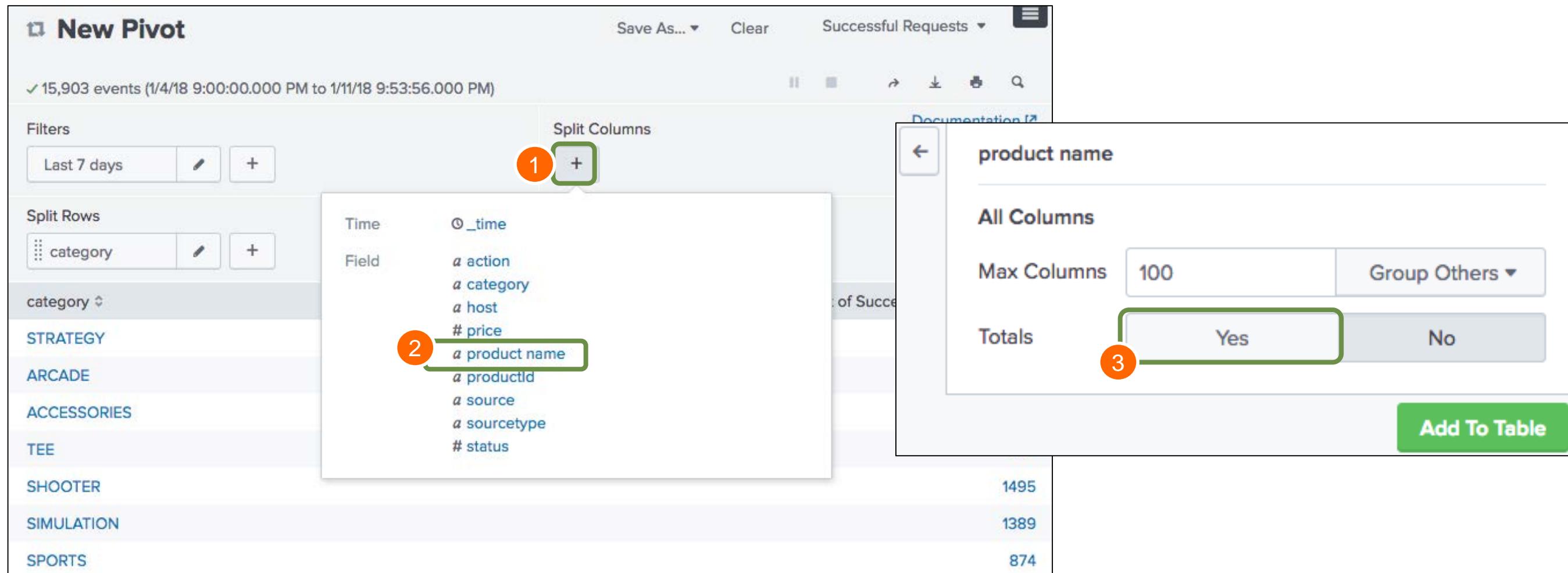
# Updated Results (with Total)



Generated for () (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 steps highlighted:

1. Click the  button under the **Split Columns** section.
2. Select the field **a product name** from the dropdown list.
3. Set the **Totals** option to **Yes**.

The interface includes a sidebar with filters for **Last 7 days**, **category**, and categories like **STRATEGY**, **ARCADE**, **ACCESSORIES**, **TEE**, **SHOOTER**, **SIMULATION**, and **SPORTS**. The main area shows a table with columns for **Time** and **Field**, and a summary table at the bottom:

|              |             | 1495 | 1389 | 874 |
|--------------|-------------|------|------|-----|
| product name | All Columns |      |      |     |
| Max Columns  | 100         |      |      |     |
| Totals       | Yes         |      |      |     |

**Add To Table** button is located at the bottom right of the dialog.

Generated for () (C) Splunk Inc, not for distribution

# Results

**New Pivot**

✓ 15,825 events (1/4/18 10:00:00.000 PM to 1/11/18 10:09:09.000 PM)

Save As... Clear Successful Requests

Filters: Last 7 days +

Split Columns: product name +

Split Rows: category +

Column Values: Count of Suc...

The ALL column shows row totals by category

| category  | Benign Space Debris | Curling 2014 | Dream Crusher | Final Sequel | Fire Resistance Suit of Provolone | Holey Blade of Gouda | Manganiello Bros. | Manganiello Bros. Tee | Mediocre Kingdoms | Orvil the Wolverine | Puppies vs. Zombies | SIM Cubicle | World of Cheese | World of Cheese Tee | ALL  |
|---|---------------------|--------------|---------------|--------------|-----------------------------------|----------------------|-------------------|-----------------------|-------------------|---------------------|---------------------|-------------|-----------------|---------------------|------|
| STRATEGY  | 0                   | 0            | 1316          | 1128         | 0                                 | 0                    | 0                 | 0                     | 1319              | 0                   | 965                 | 0           | 0               | 0                   | 4728 |
| ARCADE  | 825                 | 0            | 0             | 0            | 0                                 | 0                    | 1264              | 0                     | 0                 | 887                 | 0                   | 0           | 0               | 0                   | 2976 |
| ACCESSORIES   | 0                   | 0            | 0             | 0            | 1248                              | 1038                 | 0                 | 0                     | 0                 | 0                   | 0                   | 0           | 0               | 0                   | 2286 |
| TEE   | 0                   | 0            | 0             | 0            | 0                                 | 0                    | 0                 | 1180                  | 0                 | 0                   | 0                   | 0           | 0               | 913                 | 2093 |
| SHOOTER   | 0                   | 0            | 0             | 0            | 0                                 | 0                    | 0                 | 0                     | 0                 | 0                   | 0                   | 0           | 1490            | 0                   | 1490 |
| SIMULATION  | 0                   | 0            | 0             | 0            | 0                                 | 0                    | 0                 | 0                     | 0                 | 0                   | 0                   | 1380        | 0               | 0                   | 1380 |
| SPORTS  | 0                   | 872          | 0             | 0            | 0                                 | 0                    | 0                 | 0                     | 0                 | 0                   | 0                   | 0           | 0               | 0                   | 872  |
| <b>825    872    1316    1128    1248    1038    1264    1180    1319    887    965    1380    1490    913    15825</b> |                     |              |               |              |                                   |                      |                   |                       |                   |                     |                     |             |                 |                     |      |

The bottom (bolded) row shows column totals by product name  
Generated for () (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 image consists of two side-by-side screenshots of the Splunk interface, both titled "New Pivot".

**Left Screenshot:** Shows the initial state of the "Filters" section. It displays a time range of "Last 7 days" and a "+" button with a red circle containing the number "1". Below this, a list of fields is shown, with "a category" highlighted in green. A vertical sidebar on the right contains icons for different chart types.

**Right Screenshot:** Shows the filters being applied. The "category" field is selected, and the "Filter Type" dropdown is set to "Match". The "Match" dropdown shows "is not" selected, and the value "ACCESSORIE" is entered in the input field. A red circle labeled "4" is over the "is not" dropdown, and another red circle labeled "5" is over the "ACCESSORIE" input field. At the bottom right, a green "Add To Table" button is visible, with a red circle labeled "6" over it.

Generated for () (C) Splunk Inc, not for distribution

# Filtered Pivot

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

New Pivot

✓ 13,575 events (1/4/18 10:00:00.000 PM to 1/11/18 10:34:56.000 PM)

Save As... Clear Successful Requests

Filters

Last 7 days category is n... +

Split Columns

product name +

Split Rows

category +

Column Values

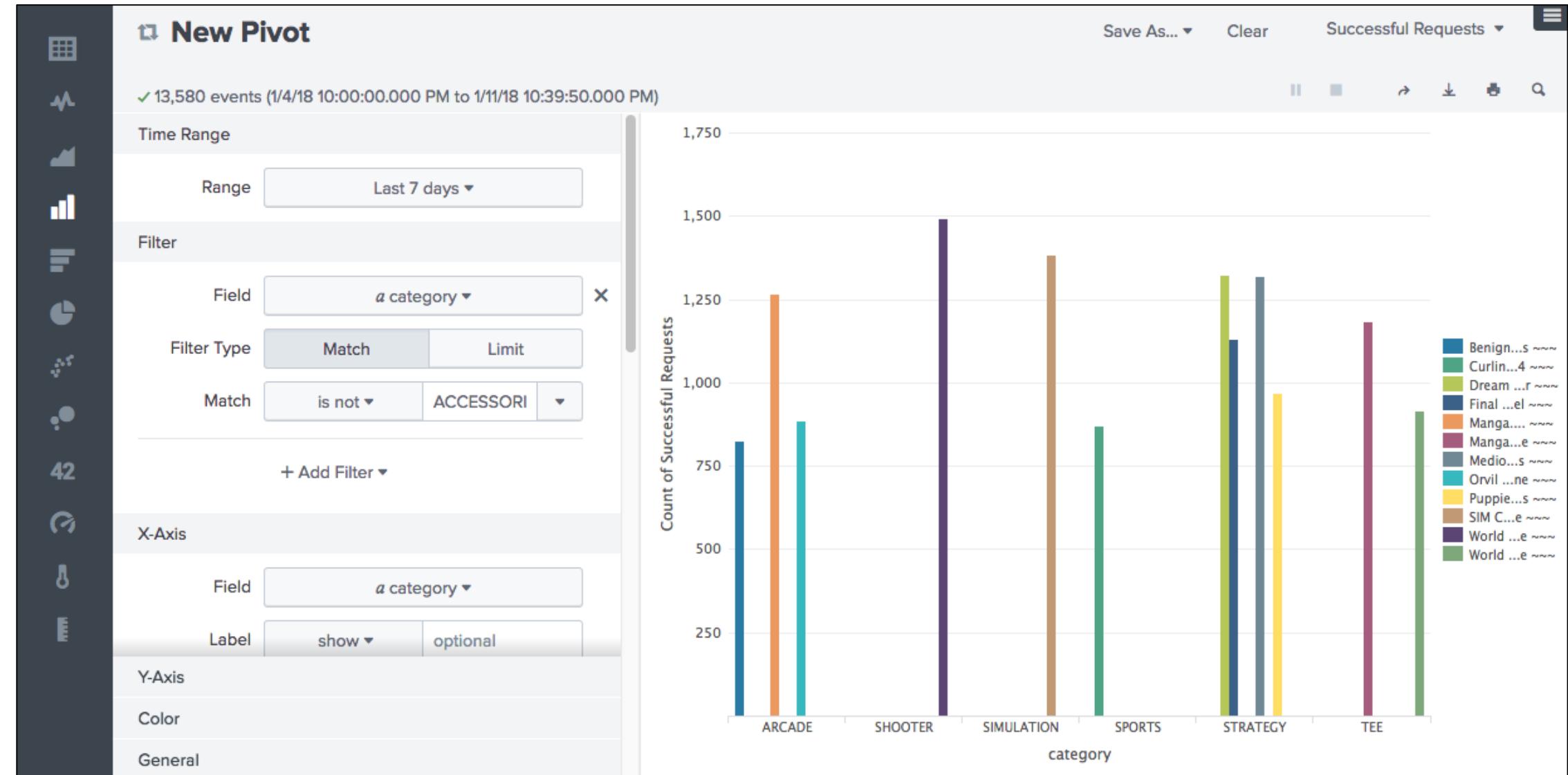
Count of Suc... +

| category   | Benign Space Debris | Curling 2014 | Dream Crusher | Final Sequel | Manganiello Bros. | Manganiello Bros. Tee | Mediocre Kingdoms | Orvil the Wolverine | Puppies vs. Zombies | SIM Cubicle | World of Cheese | World of Cheese Tee | ALL   |
|------------|---------------------|--------------|---------------|--------------|-------------------|-----------------------|-------------------|---------------------|---------------------|-------------|-----------------|---------------------|-------|
| STRATEGY   | 0                   | 0            | 1322          | 1130         | 0                 | 0                     | 1320              | 0                   | 968                 | 0           | 0               | 0                   | 4740  |
| ARCADE     | 827                 | 0            | 0             | 0            | 1266              | 0                     | 0                 | 888                 | 0                   | 0           | 0               | 0                   | 2981  |
| TEE        | 0                   | 0            | 0             | 0            | 0                 | 1186                  | 0                 | 0                   | 0                   | 0           | 0               | 917                 | 2103  |
| SHOOTER    | 0                   | 0            | 0             | 0            | 0                 | 0                     | 0                 | 0                   | 0                   | 0           | 1494            | 0                   | 1494  |
| SIMULATION | 0                   | 0            | 0             | 0            | 0                 | 0                     | 0                 | 0                   | 0                   | 1385        | 0               | 0                   | 1385  |
| SPORTS     | 0                   | 872          | 0             | 0            | 0                 | 0                     | 0                 | 0                   | 0                   | 0           | 0               | 0                   | 872   |
|            | 827                 | 872          | 1322          | 1130         | 1266              | 1186                  | 1320              | 888                 | 968                 | 1385        | 1494            | 917                 | 13575 |

Generated for () (C) Splunk Inc, not for distribution

# Select a Visualization Format

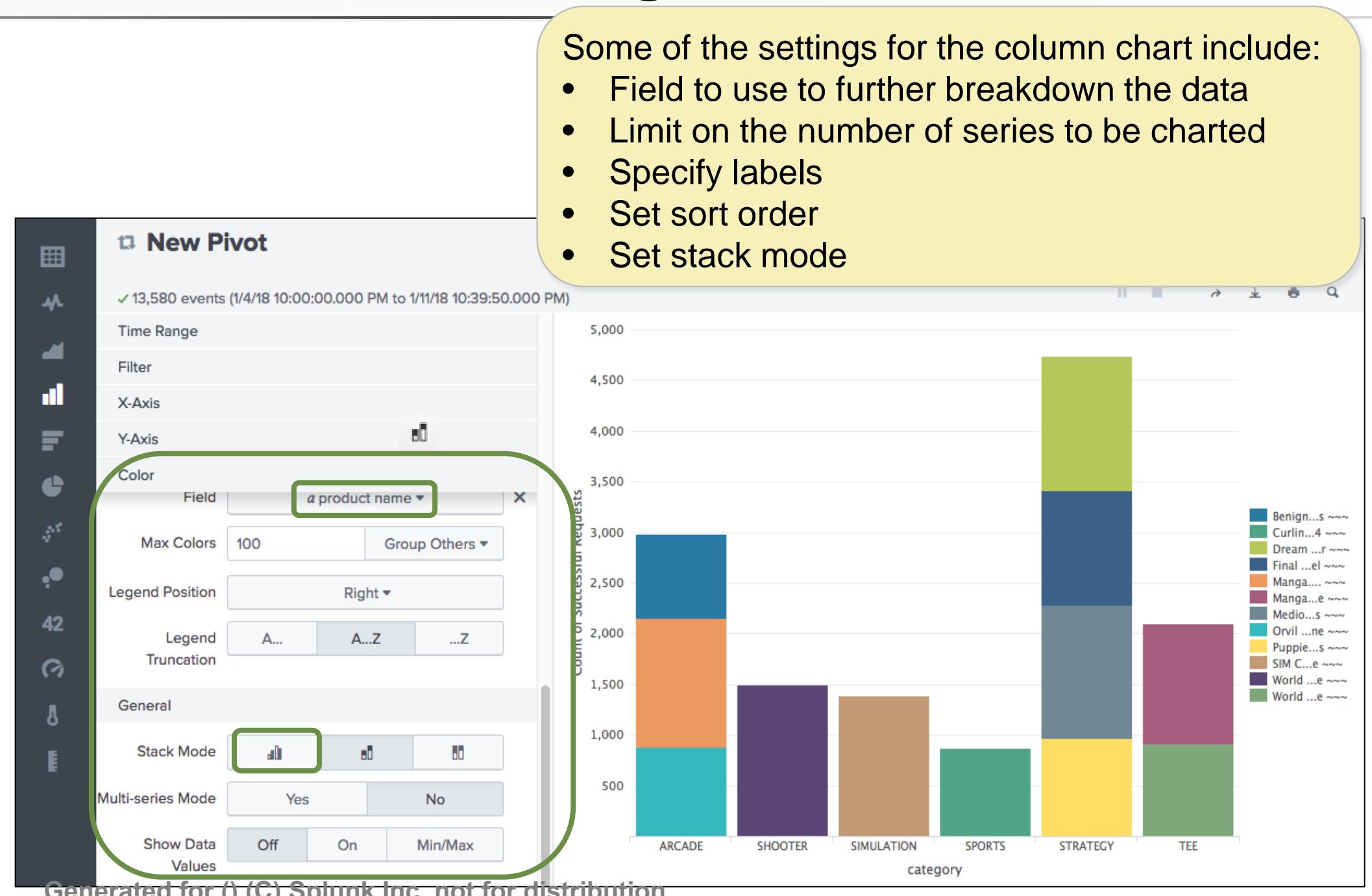
You can display your pivot as a table or a visualization, such as a column chart



Generated for () (C) Splunk Inc, not for distribution

# Modify Visualization Settings

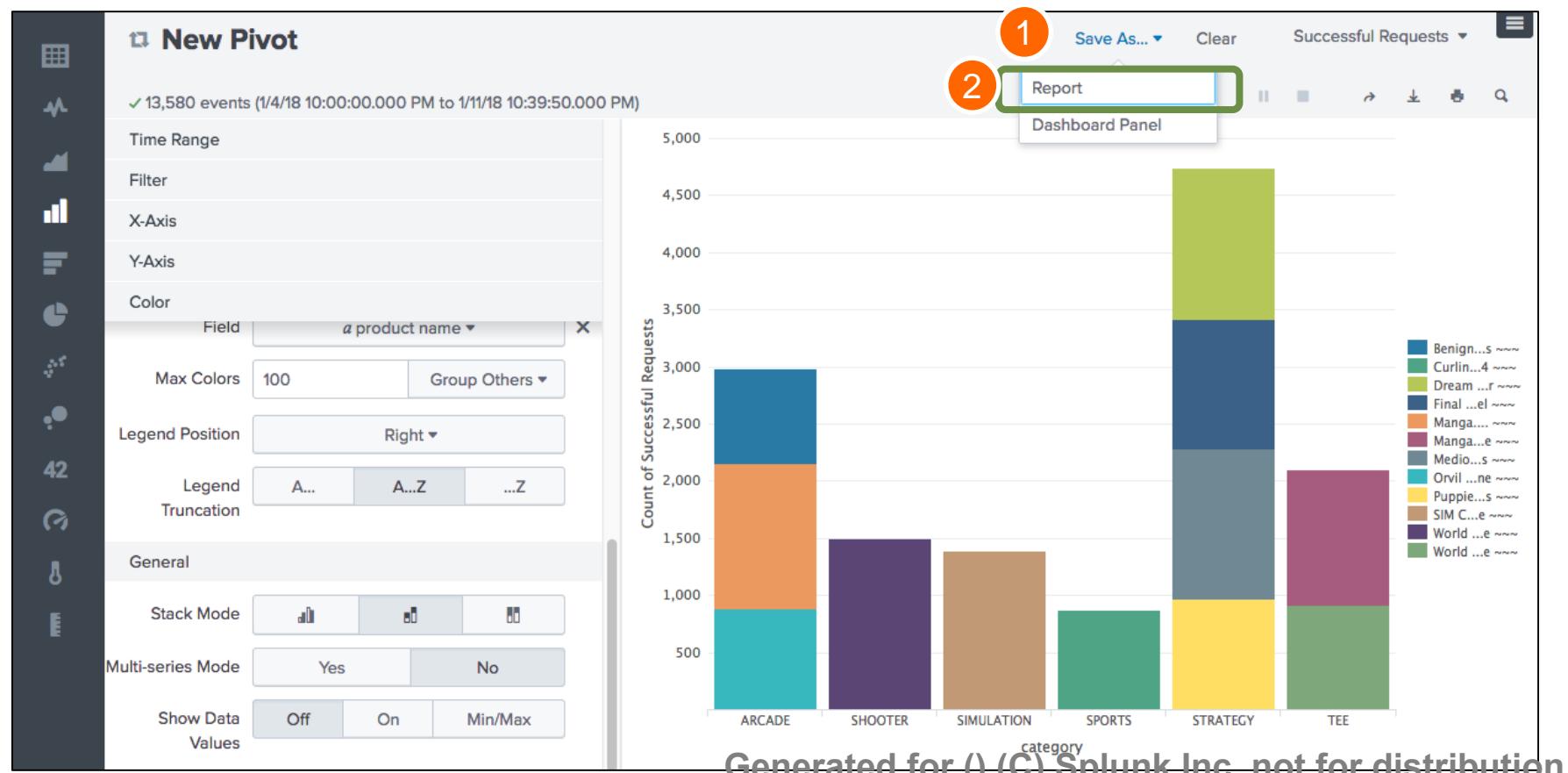
- When a visualization control is selected, panels appear that let you configure its settings
- In this example:
  - The results for each category are broken down by **product\_name**
  - The stack mode is set to stacked



Generated for () (C) Splunk Inc, not for distribution

# Saving a Pivot

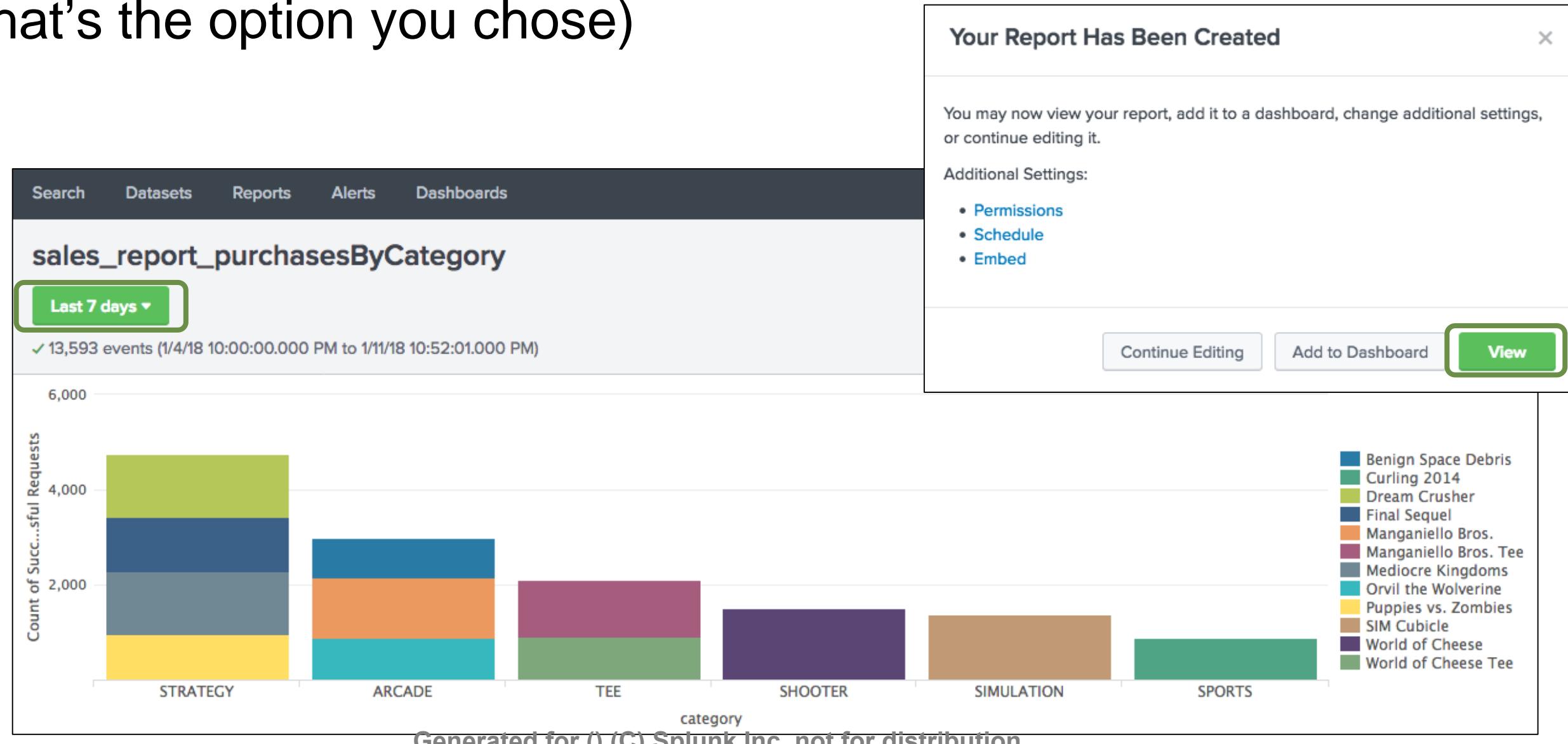
- Pivots can be saved as reports
  - You can choose to include a Time Range Picker in the report to allow people who run it to change the time range (default is Yes)



The figure shows the "Save As Report" dialog box. It has fields for "Title" (set to "sales\_report\_purchasesByCategory"), "Description" (set to "optional"), and a "Time Range Picker" switch (set to "Yes"). At the bottom are "Cancel" and "Save" buttons. Numbered circles 3 and 4 point to the "Description" field and the "Save" button respectively.

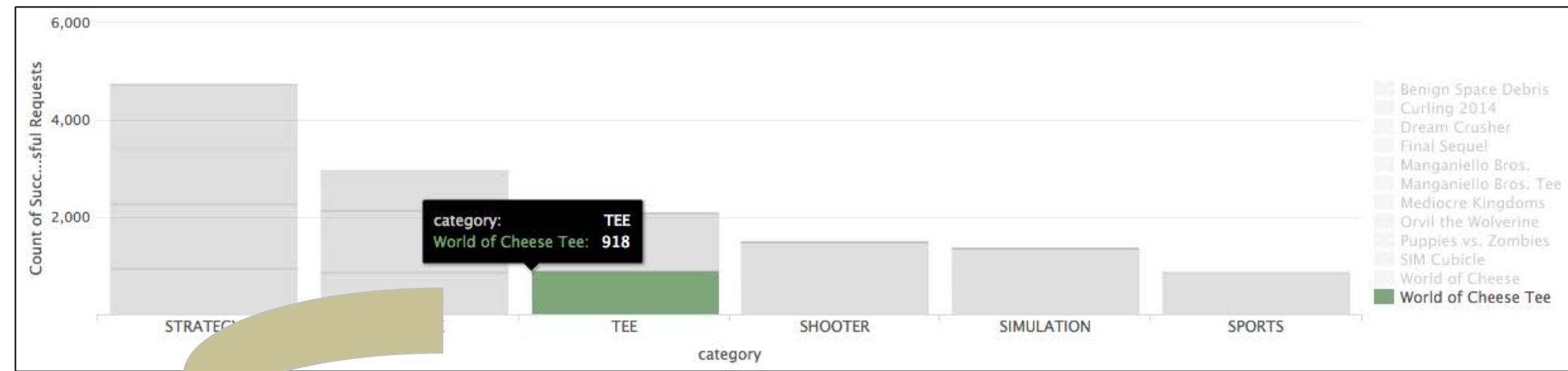
# Saving a Pivot (cont.)

When you click **View**, the report is displayed with a Time Range Picker (if that's the option you chose)



# Mouse Actions

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



**Note**

The search generated by drilldown may be more detailed than your original search. However, it produces the same results.

New Search

```
(index==* OR index=_*) (sourcetype=access_* productId="*") (categoryId!=ACCESSORIES) | search (status=200) | eval  
is_successful_purchase=if(searchmatch("(action=purchase)",1,0), 1,0), is_not_successful_purchase=1-is_successful_purchase,  
is_successful_add_to_cart=if(searchmatch("(action=addtocart)",1,0), 1,0), is_not_successful_add_to_cart=1-is_successful_add_to_cart,  
is_successful_remove=if(searchmatch("(action=remove)",1,0), 1,0), is_not_successful_remove=1-is_successful_remove | rename action AS  
http_request.action categoryId AS http_request.categoryId price AS http_request.price product_name AS http_request.product_name  
productId AS http_request.productId status AS http_request.status is_successful_purchase AS http_request.successful_request  
.is_successful_purchase is_not_successful_purchase AS http_request.successful_request.is_not_successful_purchase  
is_successful_add_to_cart AS http_request.successful_request.is_successful_add_to_cart is_not_successful_add_to_cart AS  
http_request.successful_request.is_not_successful_add_to_cart is_successful_remove AS http_request.successful_request  
.is_successful_remove is_not_successful_remove AS http_request.successful_request.is_not_successful_remove | search  
"http_request.categoryId"="TEE" "http_request.product_name"="World of Cheese Tee"
```

918 events (1/4/18 10:00:00.000 PM to 1/11/18 10:59:43.000 PM) No Event Sampling ▾ Job ▾ Verbose Mode ▾

Events (918) Patterns Statistics Visualization

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

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

< Hide Fields All Fields t Time Event

SELECTED FIELDS

1/11/18 148.107.2.20 - - [11/Jan/2018:22:49:40] "POST /cart.do?action=changeQuantity&itemId=EST-11&r

Generated for () (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
- 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 Enterprise interface with the following elements:

- Top Bar:** splunk>enterprise, App: Search & Repor..., student1, Messages, Settings, Activity, Help, Find, Search icon.
- Header:** Search, Datasets, Reports, Alerts, Dashboards, > Search & Reporting.
- Search Results:** New Search for "action=purchase".
  - Search bar: action=purchase, Yesterday.
  - Event count: 525 events (1/10/18 12:00:00.000 AM to 1/11/18 12:00:00.000 AM), No Event Sampling.
  - Job controls: Job, Smart Mode.
- Tab Selection:** Events (525) (highlighted), Patterns, Statistics (highlighted), Visualization.
- Feedback:** Your search isn't generating any statistic or visualization results. Here are some possible ways to get results.
  - Pivot:** Build tables and visualizations using multiple fields and metrics without writing searches.
  - Fields Dialog:** Which fields would you like to use as a Data Model?
    - All Fields (46)
    - Selected Fields (4)
    - Fields with at least 8 % coverage (45)
  - Search Commands:** Use a transforming search command, like timechart or stats, to summarize the data.

Generated for () (C) Splunk Inc, not for distribution

# Saving a Pivot as a Report

The screenshot shows the 'New Pivot' interface. At the top right, there is a 'Save As...' button with a dropdown menu. The 'Report' option in this menu is highlighted with a red circle containing the number '1'. Other options in the menu include 'Dashboard Panel' and 'Split Columns'. The main area of the interface displays search results for '525 events (1/10/18 12:00:00.000 AM to 1/11/18 12:00:00.000 AM)'. It includes sections for 'Filters' (with a 'Yesterday' button), 'Split Rows' (with a '+'), 'Split Columns' (with a 'host' entry), and 'Column Values' (with a 'Count of 1515...' entry).

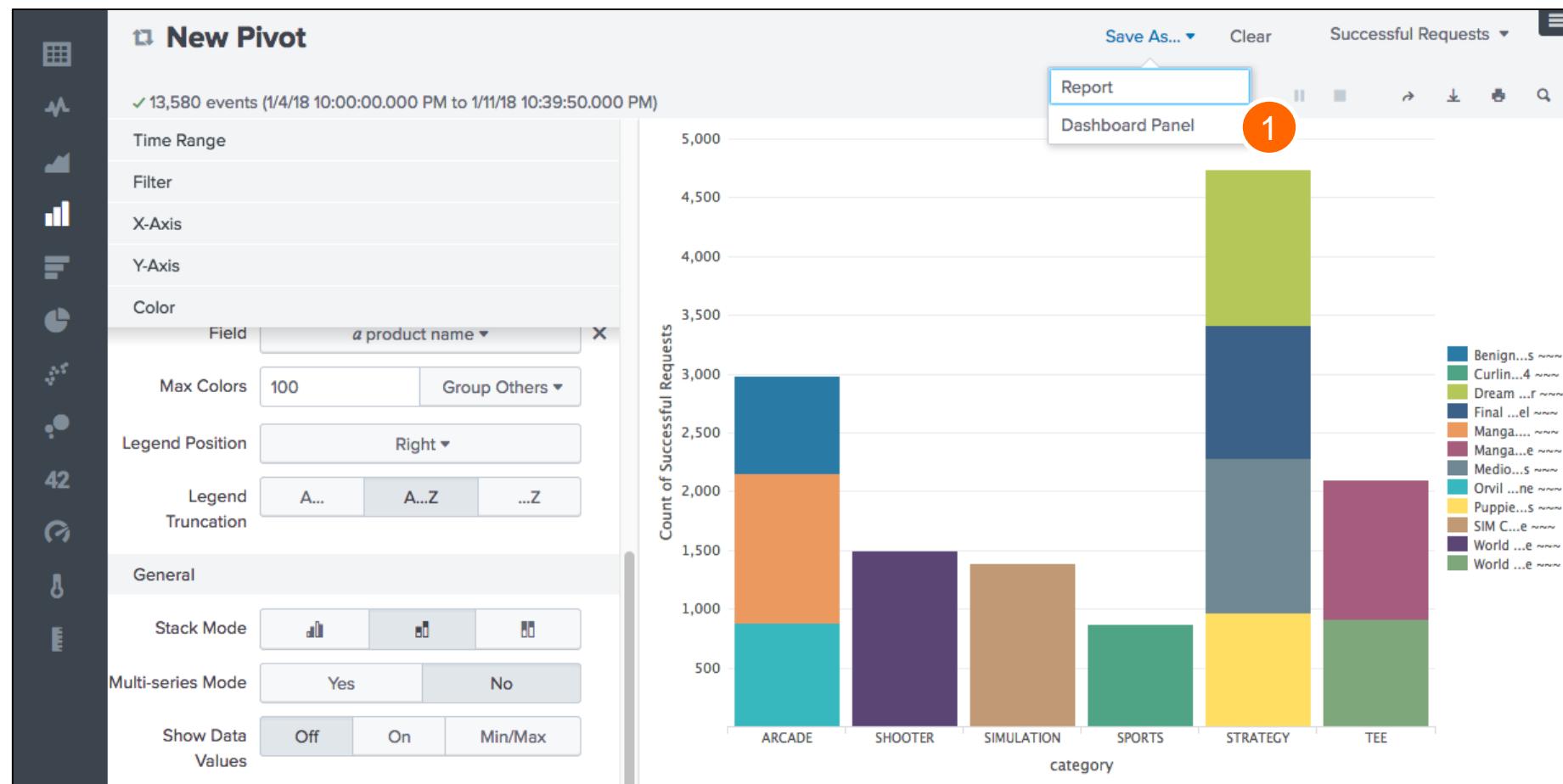
- When saving as a report, the **Model Title** is required
  - This is used to create a data model, which is required by the pivot report
- The **Model ID** is automatically generated based on the **Model Title**

The screenshot shows the 'Save As Report' dialog box. It has fields for 'Title' (set to 'sales\_report\_purchases') and 'Description' (set to 'optional'). Below these is a 'Time Range Picker' with 'Yes' selected. A note at the bottom states: 'You must save the original search as a data model. This will power the report.' The dialog is divided into three numbered sections: 1. The 'Report' option in the 'Save As...' dropdown of the New Pivot interface. 2. The 'Model Title' field in the Save As Report dialog set to 'purchase data model'. 3. The 'Save' button in the bottom right corner of the dialog.

**Note**   
Manually changing the Model ID is not recommended.

# Add a Pivot to a Dashboard

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



Save As Dashboard Panel

Dashboard

New Existing

Dashboard Title: Buttercup Sales Week

Dashboard ID: buttercup\_sales\_week\_

Can only contain letters, numbers and underscores.

Dashboard Description: optional

Dashboard Permissions

Private Shared in App

Panel Title: optional

Panel Powered By

Inline Search Report

Drilldown: No action

Panel Content

Statistics Column Chart

Cancel Save

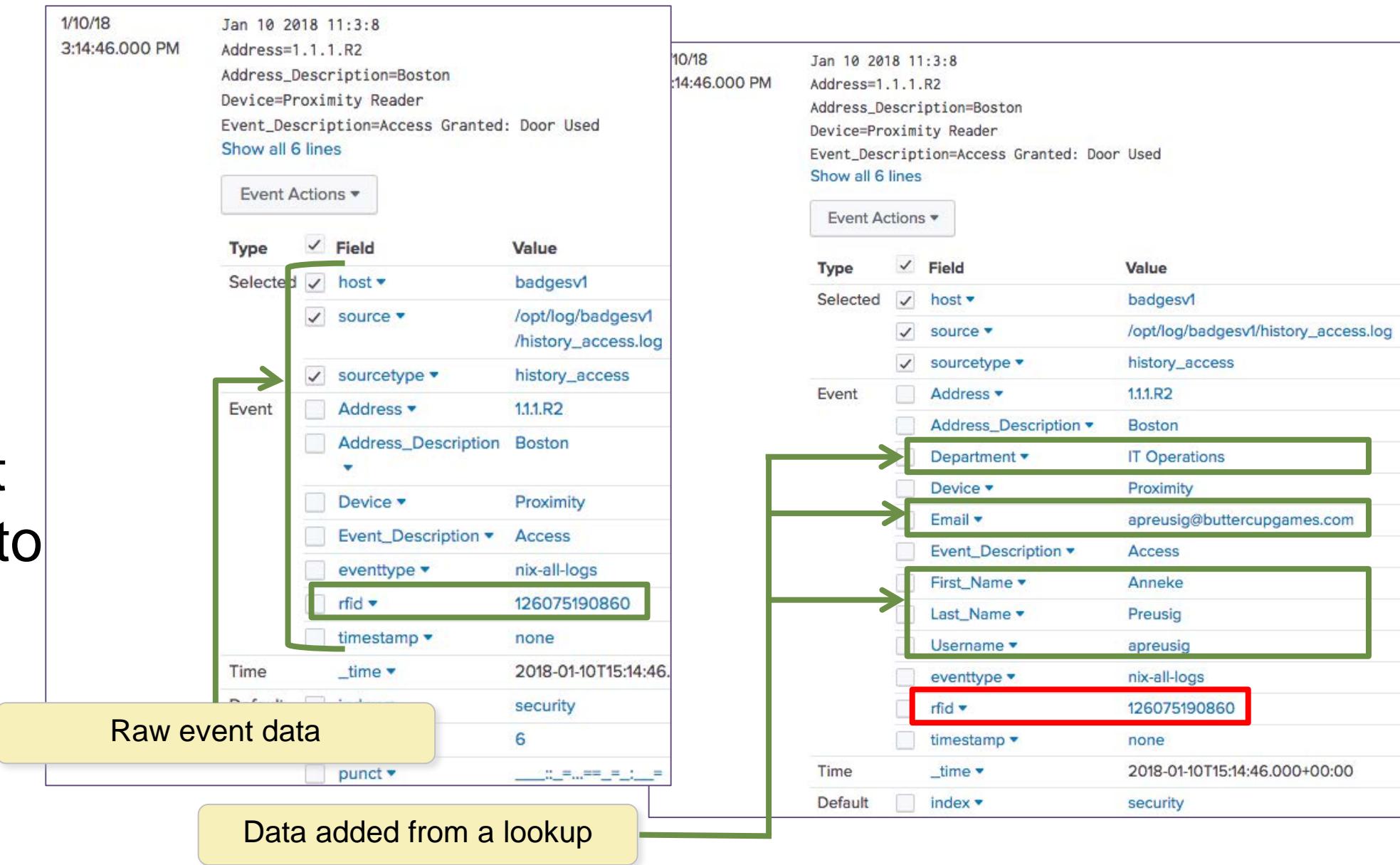
Generated for () (C) Splunk Inc, not for distribution

# Module 12: Creating and Using Lookups

Generated for () (C) Splunk Inc, not for distribution

# What Is a Lookup?

- Sometimes static (or relatively unchanging) data is required for searches, but isn't available in the index
- Lookups pull such data from standalone files at search time and add it to search results



Generated for () (C) Splunk Inc, not for distribution

# What Is a Lookup? (cont.)

- Lookups allow you to add more fields to your events, such as:
  - Descriptions for HTTP status codes (“File Not Found”, “Service Unavailable”)
  - Sale prices for products
  - User names, IP addresses, and workstation IDs associated with RFIDs
- After a 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

**Note**   
Admins can change the `case_sensitive_match` option to `false` in `transforms.conf`

# A Sample Lookup File

- 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

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

The screenshot shows the 'Lookups' page in the Splunk UI. The title 'Lookups' is at the top, followed by the subtitle 'Create and configure lookups.' Below this are three main sections, each with a numbered callout (1, 2, or 3) and a ' + Add new' button:

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

Generated for () (C) Splunk Inc, not for distribution

# Adding a New Lookup Table File

## Settings > Lookups > Lookup table files

1. Click **New Lookup Table File**
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

2 Destination app search

3 Upload a lookup file  Products.csv  
Select either a plaintext CSV file, a gzipped CSV file, or a KMZ/KML file.  
The maximum file size that can be uploaded through the browser is 500MB.

4 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/KML file, we recommend a filename ending in ".kmz"/".kml".

5

Generated for () (C) Splunk Inc, not for distribution

# 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.

New Search Save As ▾ Close

| `inputlookup products.csv` Last 24 hours ▾ 

✓ 14 results (1/8/18 10:00:00.000 PM to 1/9/18 10:36:03.000 PM) No Event Sampling ▾ Job ▾  Smart Mode ▾

Events Patterns Statistics (14) Visualization

20 Per Page ▾ Format 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 | Holey Blade of Gouda              | 2.99       |
| N    | ACCESSORIES | 3.99  | WC-SH-A02 | Fire Resistance Suit of Provolone | 1.99       |

Generated for () (C) Splunk Inc, not for distribution

# Creating a Lookup Definition

## Settings > Lookups > Lookup definitions

1. Click New Lookup Definition
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

|   |                 |                |
|---|-----------------|----------------|
| 2 | Destination app | search         |
| 3 | Name *          | product_lookup |
| 4 | Type            | File-based     |
| 5 | Lookup file *   | products.csv   |

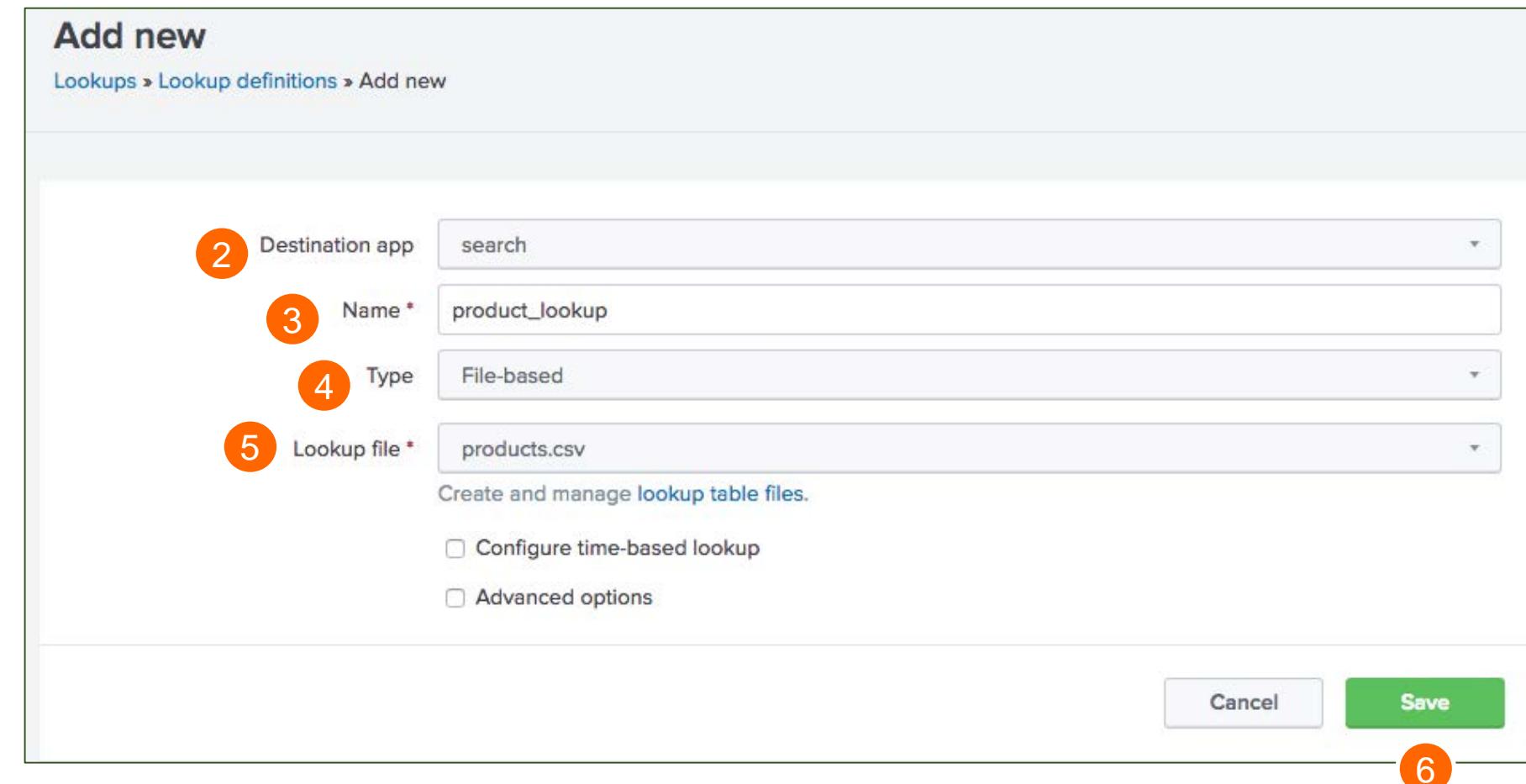
Create and manage [lookup table files](#).

Configure time-based lookup

Advanced options

[Cancel](#) [Save](#)

6



Generated for () (C) Splunk Inc, not for distribution

# Applying Advanced Lookup Options

- Min/max # of matches for each input lookup value
- Default value to output (when fewer than the min # of matches present for a given input)
- Case sensitivity match on/off
- Batch index query: improves performance for large lookup files
- Match type: supplies format for non-exact matching
- Filter lookup: filters results before returning data

The screenshot shows the 'Advanced options' configuration page in Splunk. It includes fields for 'Minimum matches' (set to 1), 'Maximum matches' (set to 'other'), 'Default matches' (set to 'other'), 'Case sensitive match' (checked), 'Batch index query' (unchecked), 'Match type' (unchecked), and 'Filter lookup' (unchecked). A 'Configure time-based lookup' checkbox is also present but unchecked.

# lookup Command

- If a lookup is not configured to run automatically, use the `lookup` command in your search to use the lookup fields
- The `OUTPUT` argument is optional
  - If `OUTPUT` not specified, `lookup` returns all the fields from the lookup table except the match 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

```
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 

497 events (1/8/18 11:00:00.000 PM to 1/9/18 11:10:56.000 PM) No Event Sampling Job Smart Mode

Events Patterns Statistics (14) Visualization

20 Per Page Format Preview

| product_name                      | sales  |
|-----------------------------------|--------|
| Benign Space Debris               | 274.89 |
| Curling 2014                      | 319.84 |
| Dream Crusher                     | 879.78 |
| Final Sequel                      | 599.76 |
| Fire Resistance Suit of Provolone | 87.78  |
| Holey Blade of Gouda              | 137.77 |
| Manganiello Bros.                 | 679.83 |
| Manganiello Bros. Tee             | 219.78 |
| Mediocre Kingdoms                 | 499.80 |
| Orvil the Wolverine               | 439.89 |
| Puppies vs. Zombies               | 74.85  |
| SIM Cubicle                       | 379.81 |
| World of Cheese                   | 449.82 |
| World of Cheese Tee               | 129.87 |

Scenario 

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

Generated for () (C) Splunk Inc, not for distribution

# Creating an Automatic Lookup

Settings > Lookups > Automatic lookups

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

Add new

Lookups > Automatic lookups > Add new

2 Destination app search

3 Name \* product\_auto\_lookup

4 Lookup table \* product\_lookup

5 Apply to sourcetype named \* access\_combined

Generated for () (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

The screenshot shows the 'Lookup input fields' and 'Lookup output fields' sections of the Splunk UI. In the 'Lookup input fields' section, 'productId' is listed with a green arrow pointing up to 'column name in lookup' and another green arrow pointing down to 'field name in Splunk'. In the 'Lookup output fields' section, 'categoryId' is listed with a green arrow pointing up to 'file' and another green arrow pointing down to 'D'. A legend at the top identifies the colors: A is light blue, B is light orange, C is light green, and D is light purple. Buttons for 'Cancel' and 'Save' are at the bottom right.

- D. Name you want displayed in Splunk; otherwise it inherits the column name

## 7. Save

Generated for () (C) Splunk Inc, not for distribution

# 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. At the top, a search bar contains the command:

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

The search results show a table of sales data. A specific row for productId "DC-SG-G02" is highlighted with a green box. An arrow points from this row to a secondary table on the right, which contains product details like price, productId, and product\_name. Another arrow points back from the secondary table to the main table's sales column for the same row.

| i | Time                      | Event   | price | productId | product_name        |
|---|---------------------------|---|-------|-----------|---------------------|
| > | 1/9/18<br>10:56:54.000 PM | 203.45.206.135 - - [09/Jan/2018:22:56:54] "POST /cart.do?action=purchase&itemId=EST-19&JSESSIONID=SD5SL5<br>FF10ADFF4951 HTTP 1.1" 200 1427 "http://www.buttercupgames.com/cart.do?action=addtocart&i<br>tegoryId=STRATEGY&productId=DC-SG-G02" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) Ap<br>(KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 314<br>host = www.buttercupgames.com<br>productId = DC-SG-G02 | 24.99 | DB-SG-G01 | Mediocre Kingdoms   |
| > | 1/9/18<br>10:56:08.000 PM | 203.45.206.135 - - [09/Jan/2018:22:56:08] "POST /cart.do?action=purchase&itemId=EST-7&JSE<br>SSIONID=SD5SL5 HTTP 1.1" 200 1427 "http://www.buttercupgames.com/cart.do?action=addtocart&i<br>tegoryId=STRATEGY&productId=DC-SG-G02" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) Ap<br>(KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 314<br>host = www.buttercupgames.com<br>productId = DC-SG-G02              | 39.99 | DC-SG-G02 | Dream Crusher       |
|   |                           | Events Patterns Statistics (14) Visualization   | 24.99 | FS-SG-G03 | Final Sequel        |
|   |                           | 20 Per Page ▾ Format Preview ▾  | 24.99 | WC-SH-G04 | World of Cheese     |
|   |                           | productId ◁   | 9.99  | WC-SH-T02 | World of Cheese Tee |
|   |                           | product_name ◁  |       |           |                     |
|   |                           | sales ◁   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           |   |       |           |                     |
|   |                           | Generated for () (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 December and January and calculated the sales based on the correct unit price for those dates

| product_time | productId | product_name                      | categoryId  | price | sale_price |
|--------------|-----------|-----------------------------------|-------------|-------|------------|
| 12/1/17      | DB-SG-G01 | Mediocre Kingdoms                 | STRATEGY    | 24.99 | 19.99      |
| 12/1/17      | DC-SG-G02 | Dream Crusher                     | STRATEGY    | 39.99 | 24.99      |
| 12/1/17      | FS-SG-G03 | Final Sequel                      | STRATEGY    | 24.99 | 16.99      |
| 12/1/17      | WC-SH-G04 | World of Cheese                   | SHOOTER     | 24.99 | 19.99      |
| 12/1/17      | WC-SH-T02 | World of Cheese Tee               | TEE         | 9.99  | 6.99       |
| 12/1/17      | PZ-SG-G05 | Puppies vs. Zombies               | STRATEGY    | 4.99  | 1.99       |
| 12/1/17      | CU-PG-G06 | Curling 2014                      | SPORTS      | 19.99 | 16.99      |
| 12/1/17      | MB-AG-G07 | Manganiello Bros.                 | ARCADE      | 39.99 | 24.99      |
| 12/1/17      | MB-AG-T01 | Manganiello Bros. Tee             | TEE         | 9.99  | 6.99       |
| 12/1/17      | FI-AG-G08 | Orvil the Wolverine               | ARCADE      | 39.99 | 24.99      |
| 12/1/17      | BS-AG-G09 | Benign Space Debris               | ARCADE      | 24.99 | 19.99      |
| 12/1/17      | SC-MG-G10 | SIM Cubicle                       | SIMULATION  | 19.99 | 16.99      |
| 12/1/17      | WC-SH-A01 | Holey Blade of Gouda              | ACCESSORIES | 5.99  | 2.99       |
| 12/1/17      | WC-SH-A02 | Fire Resistance Suit of Provolone | ACCESSORIES | 3.99  | 1.99       |
| 1/1/18       | DB-SG-G01 | Mediocre Kingdoms                 | STRATEGY    | 24.99 | 19.99      |
| 1/1/18       | DC-SG-G02 | Dream Crusher                     | STRATEGY    | 40.99 | 24.99      |
| 1/1/18       | FS-SG-G03 | Final Sequel                      | STRATEGY    | 25.99 | 16.99      |
| 1/1/18       | WC-SH-G04 | World of Cheese                   | SHOOTER     | 24.99 | 19.99      |
| 1/1/18       | WC-SH-T02 | World of Cheese Tee               | TEE         | 9.99  | 6.99       |
| 1/1/18       | PZ-SG-G05 | Puppies vs. Zombies               | STRATEGY    | 4.99  | 1.99       |
| 1/1/18       | CU-PG-G06 | Curling 2014                      | SPORTS      | 20.99 | 16.99      |
| 1/1/18       | MB-AG-G07 | Manganiello Bros.                 | ARCADE      | 39.99 | 24.99      |
| 1/1/18       | MB-AG-T01 | Manganiello Bros. Tee             | TEE         | 9.99  | 6.99       |
| 1/1/18       | FI-AG-G08 | Orvil the Wolverine               | ARCADE      | 39.99 | 24.99      |
| 1/1/18       | BS-AG-G09 | Benign Space Debris               | ARCADE      | 25.99 | 19.99      |
| 1/1/18       | SC-MG-G10 | SIM Cubicle                       | SIMULATION  | 19.99 | 16.99      |
| 1/1/18       | WC-SH-A01 | Holey Blade of Gouda              | ACCESSORIES | 6.99  | 2.99       |
| 1/1/18       | WC-SH-A02 | Fire Resistance Suit of Provolone | ACCESSORIES | 4.99  | 1.99       |

| product_name                 | Month | price | count | sales      | SubTotal Sales |
|------------------------------|-------|-------|-------|------------|----------------|
| Benign Space Debris          | Dec   | 24.99 | 828   | 42,211.44  |                |
| Benign Space Debris          | Jan   | 25.99 | 646   | 32,933.08  |                |
| Benign Space Debris Subtotal |       |       |       |            | 150,289.04     |
| Curling 2014                 | Dec   | 19.99 | 868   | 35,570.64  |                |
| Curling 2014                 | Jan   | 20.99 | 620   | 25,407.60  |                |
| Curling 2014 Subtotal        |       |       |       |            | 121,956.48     |
| Dream Crusher                | Dec   | 39.99 | 1,360 | 110,132.80 |                |
| Dream Crusher                | Jan   | 40.99 | 1,004 | 81,303.92  |                |
| Dream Crusher Subtotal       |       |       |       |            | 382,873.44     |
| Final Sequel                 | Dec   | 24.99 | 1,200 | 61,176.00  |                |
| Final Sequel                 | Jan   | 25.99 | 812   | 41,395.76  |                |
| Final Sequel Subtotal        |       |       |       |            | 205,143.52     |

Generated for () (C) Splunk Inc, not for distribution

# Module 13

# Creating Scheduled Reports and Alerts

Generated for () (C) Splunk Inc, not for distribution

# Why Scheduled Reports?

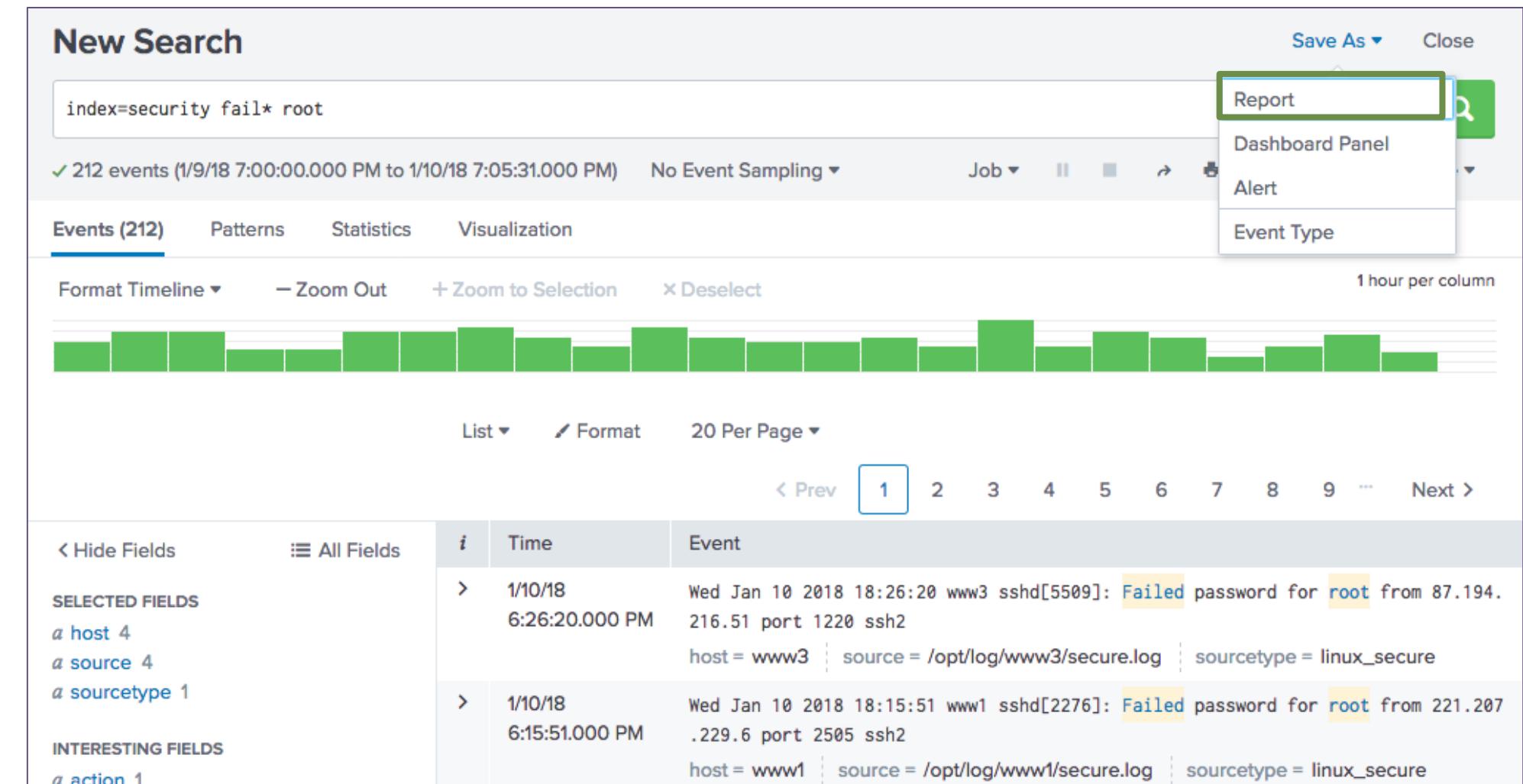
---

Scheduled Reports are useful for:

- Monthly, weekly, daily executive/managerial roll up reports
- Dashboard performance
- Automatically sending reports via email

# Creating a Scheduled Report

1. Create your search
2. From the Save As menu, select Report



Generated for () (C) Splunk Inc, not for distribution

# Creating a Scheduled Report (cont.)

3. Enter Title
4. Enter Description
5. Set Time Range Picker to No
6. Click Save

Save As Report

|                   |   |
|-------------------|---|
| Title             | IT_Report_FailedRootLogins                                    |
| Description       | linux_secure failed root logins                               |
| Content           | Events  |
| Time Range Picker | <input type="radio"/> Yes <input checked="" type="radio"/> No |

**Cancel** **Save**

Note 

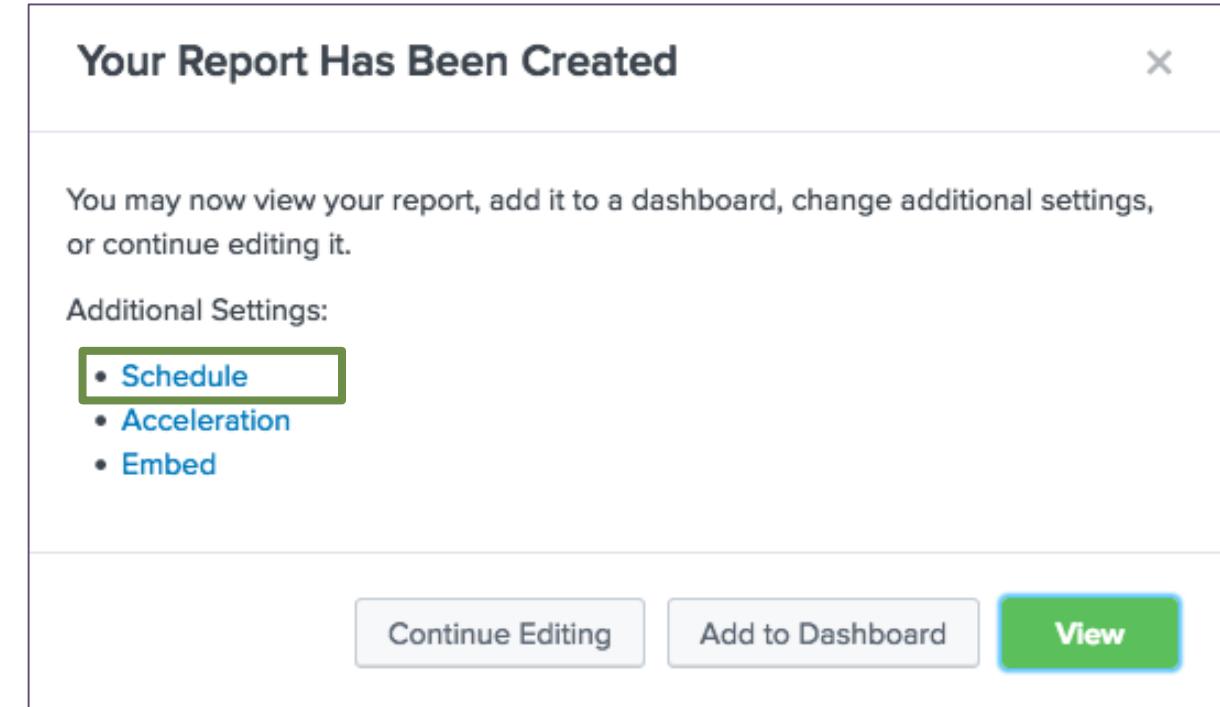
Time Range Picker cannot be used with scheduled reports.

# Creating a Scheduled Report (cont.)

- After the report is created, click Schedule
- If you inadvertently set Time Range Picker to Yes on previous screen, a warning displays and time picker is disabled



Scheduling this report results in removal of the time picker from the report display.



## Note



Depending on the permissions granted to you by your Splunk administrator, you may be able to set permissions to share your scheduled report.

# 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 IT\_Report\_FailedRootLogins

Schedule Report  Learn More ↗

Schedule Run every week ▾

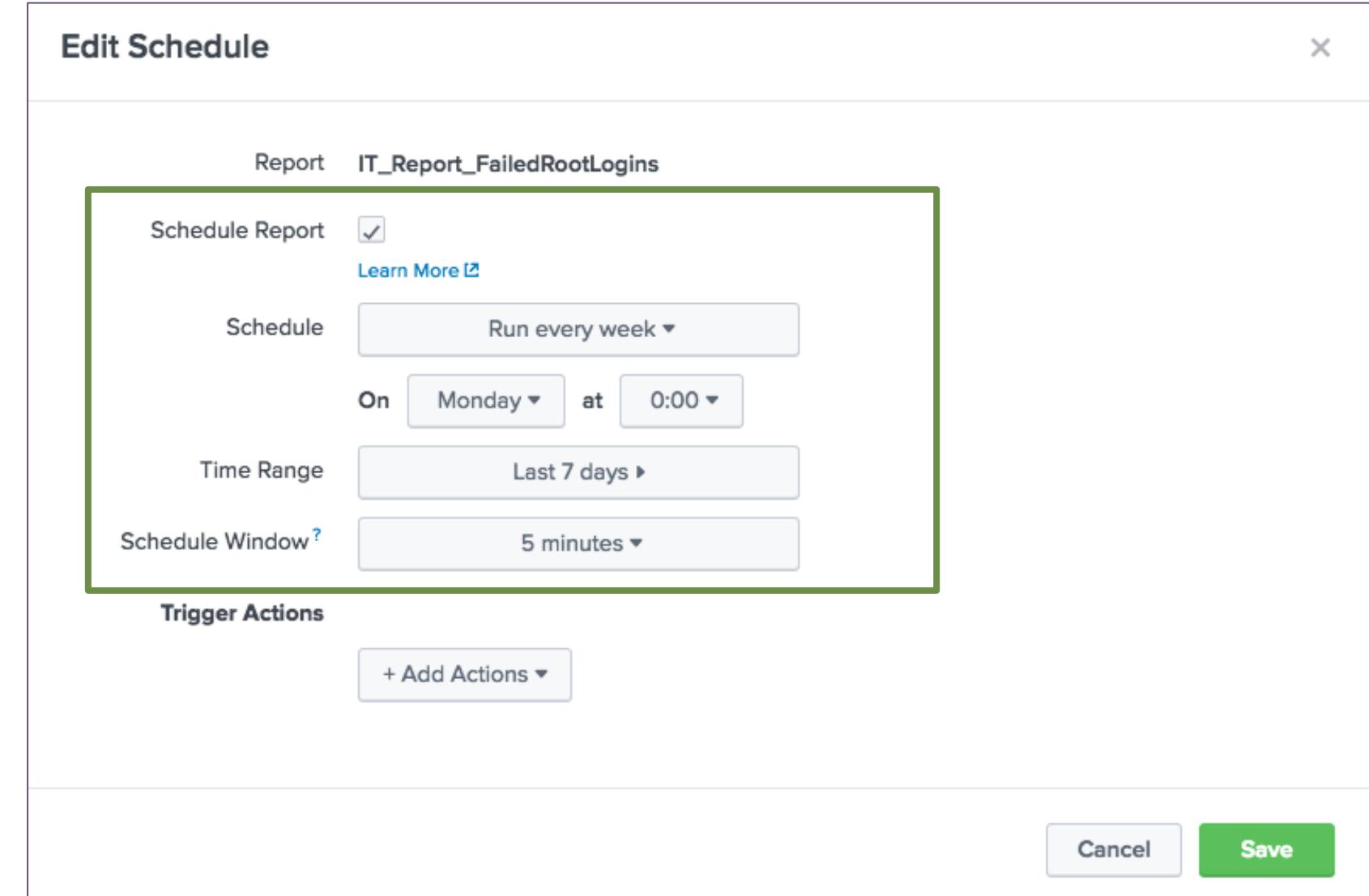
On Monday at 0:00

Time Range Last 7 days ▶

Schedule Window ? 5 minutes ▾

Trigger Actions + Add Actions ▾

Cancel Save



Generated for () (C) Splunk Inc, not for distribution

# Creating a Scheduled Report – Select Time Range

- Time Range – By default, search time range 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

Edit Schedule

Report IT\_Report\_FailedRootLogins

Schedule Report  [Learn More](#)

Schedule Run every week

On Monday at 0:00

Time Range Last 7 days

Schedule Window 5 minutes

Trigger Actions + Add Actions

Note [i](#)

Users with admin privileges can also select a Schedule Priority of Default, Higher, or Highest.

Select Time Range

Presets

| RELATIVE               | OTHER           |
|------------------------|-----------------|
| Today                  | Last 15 minutes |
| Week to date           | Last 60 minutes |
| Business week to date  | Last 4 hours    |
| Month to date          | Last 24 hours   |
| Year to date           | Last 7 days     |
| Yesterday              | Last 30 days    |
| Previous week          | All time        |
| Previous business week |                 |
| Previous month         |                 |
| Previous year          |                 |

> Relative

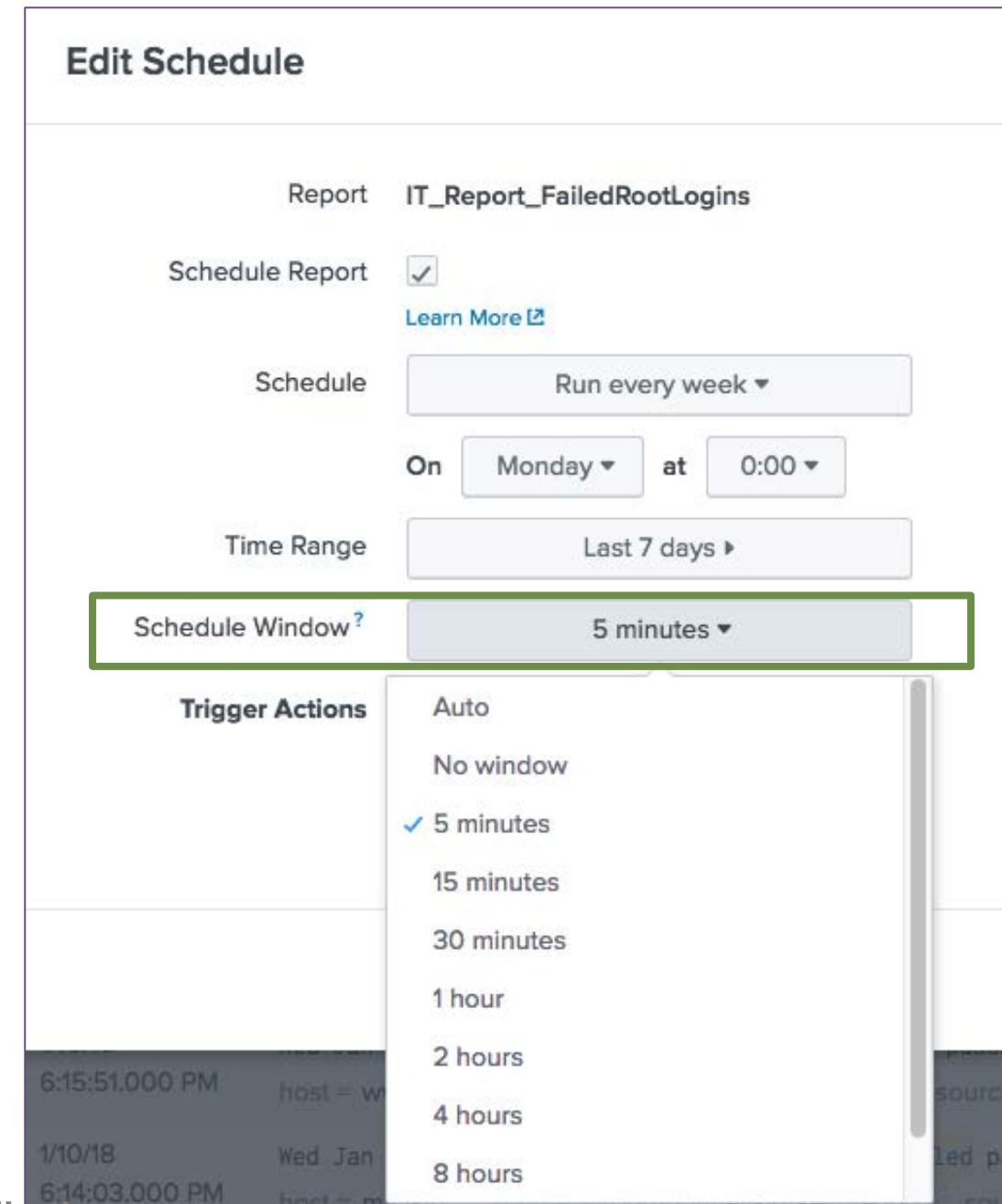
> Advanced

Back

Generated for () (C) Splunk Inc, not for distribution

# Creating a Scheduled Report – Schedule Window

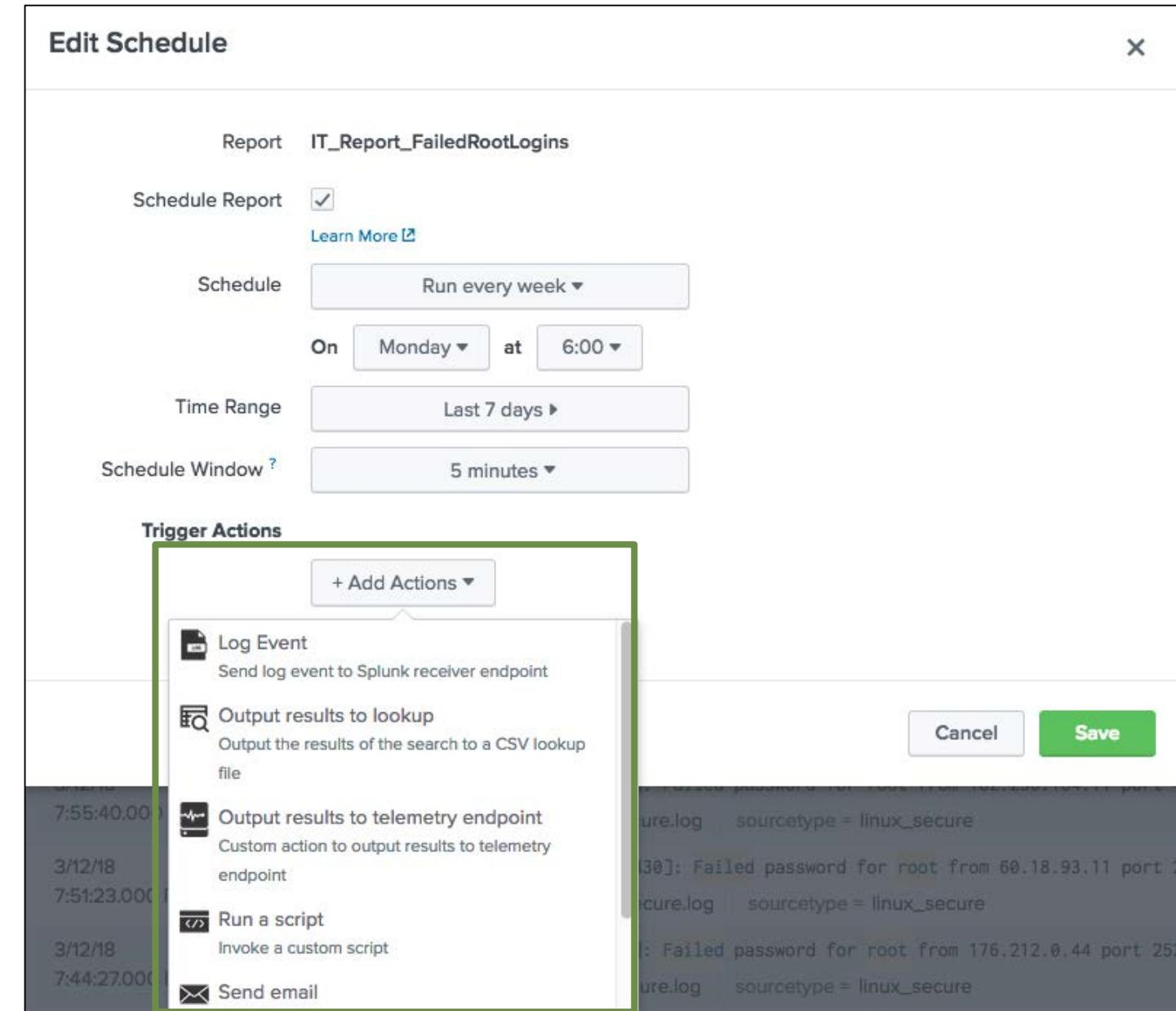
- Schedule Window – this setting determines a time frame to run the report
  - If there are other reports scheduled to run at the same time, you can provide a window in which to run the report
  - This setting provides efficiency when scheduling several reports to run
- After you configure the report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



Generated for () (C) Splunk Inc, not for distribution

# Creating a Scheduled Report – Add Actions

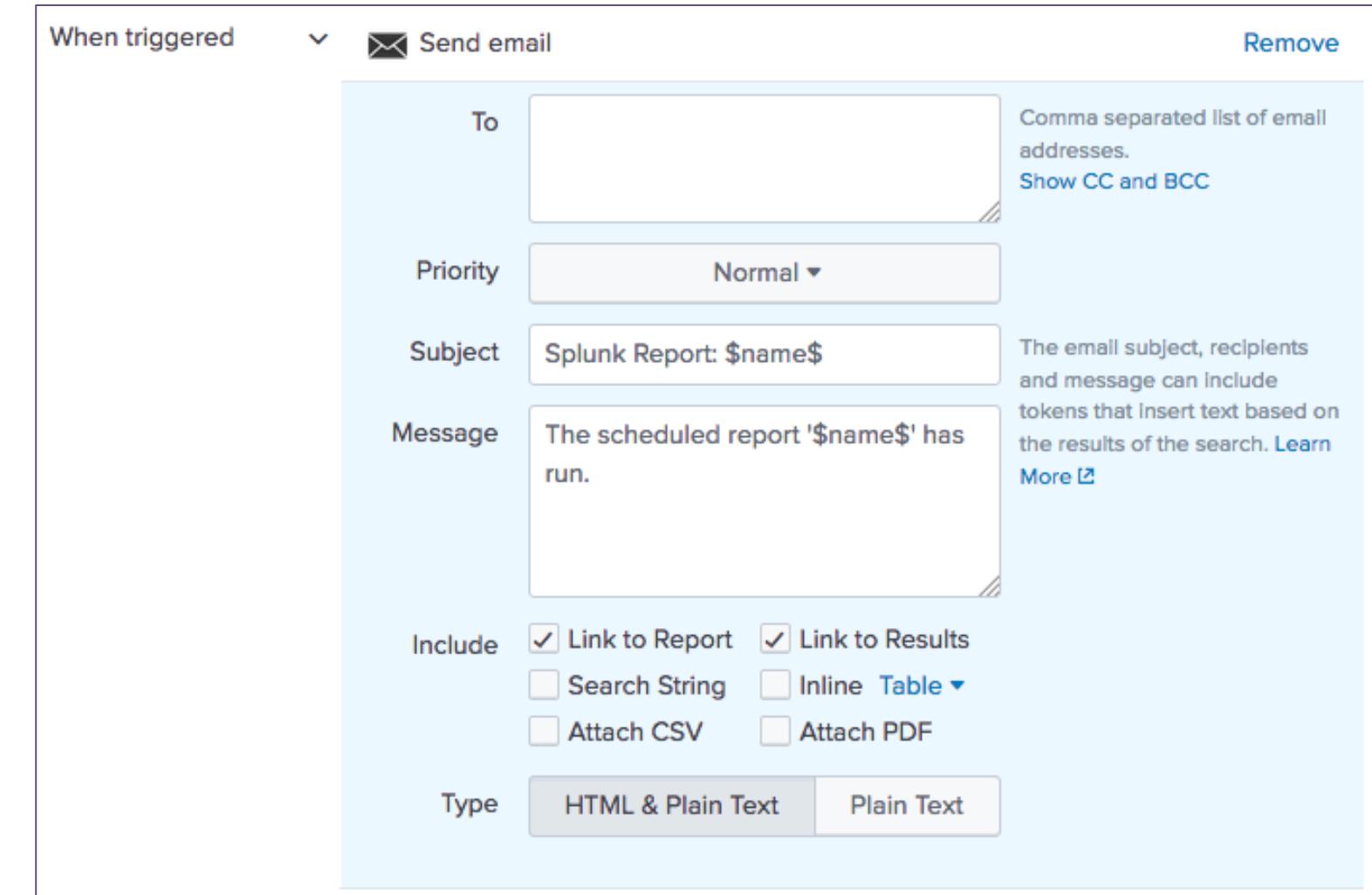
- **Log Event** – creates an indexed, searchable log event
- **Output results to lookup** – sends results of search to CSV lookup file
- **Output results to telemetry endpoint** – sends usage metrics back to Splunk (if your company has opted-in to program)
- **Run a script** – runs a previously created script
- **Send email** – sends an email with results to specified recipients
- **Webhook** – sends an HTTP POST request to specified URL



Generated for () (C) Splunk Inc, not for distribution

# Creating a Scheduled Report – Send Email

1. Enter addresses in the To field, separated by commas
2. Set the priority
3. Edit or keep the default subject  
The \$name\$ variable includes the name of the report
4. If desired, include other options, such as an inline table of results
5. Define the email text type
6. Click Save



Generated for () (C) Splunk Inc, not for distribution

# Managing Reports – Edit Permissions

**Reports**

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.

1 Reports

| Title                      | Actions               | Next Scheduled Time | Owner    | App         | Sharing |
|----------------------------|-----------------------|---------------------|----------|-------------|---------|
| IT_Report_FailedRootLogins | Open in Search Edit ▾ | None                | student1 | class_Fund1 | Private |

**Edit Description**

**Edit Permissions** (highlighted with a green box)

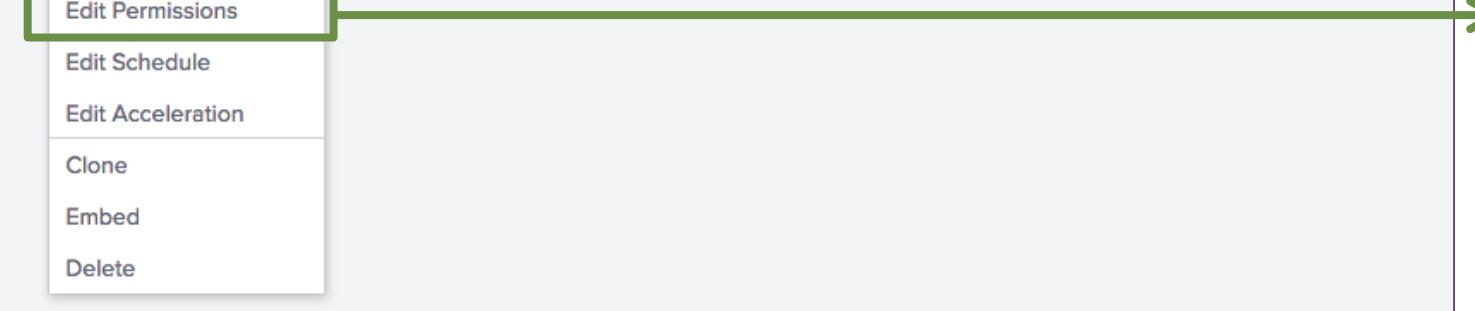
**Edit Schedule**

**Edit Acceleration**

**Clone**

**Embed**

**Delete**



**Edit Permissions**

Report **IT\_Report\_FailedRootLogins**

Owner **student1**

App **class\_Fund1**

Display For **Owner** (highlighted with a green box)

Run As **Owner**

Learn More ↗

|                    | Read                     | Write                    |
|--------------------|--------------------------|--------------------------|
| Everyone           | <input type="checkbox"/> | <input type="checkbox"/> |
| admin              | <input type="checkbox"/> | <input type="checkbox"/> |
| can_delete         | <input type="checkbox"/> | <input type="checkbox"/> |
| power              | <input type="checkbox"/> | <input type="checkbox"/> |
| splunk-system-role | <input type="checkbox"/> | <input type="checkbox"/> |
| student            | <input type="checkbox"/> | <input type="checkbox"/> |
| user               | <input type="checkbox"/> | <input type="checkbox"/> |
| windows-admin      | <input type="checkbox"/> | <input type="checkbox"/> |

**Note**

The proper permissions from your Splunk administrator are required to edit the permissions on a scheduled report.

**Cancel** **Save**

Generated for () (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

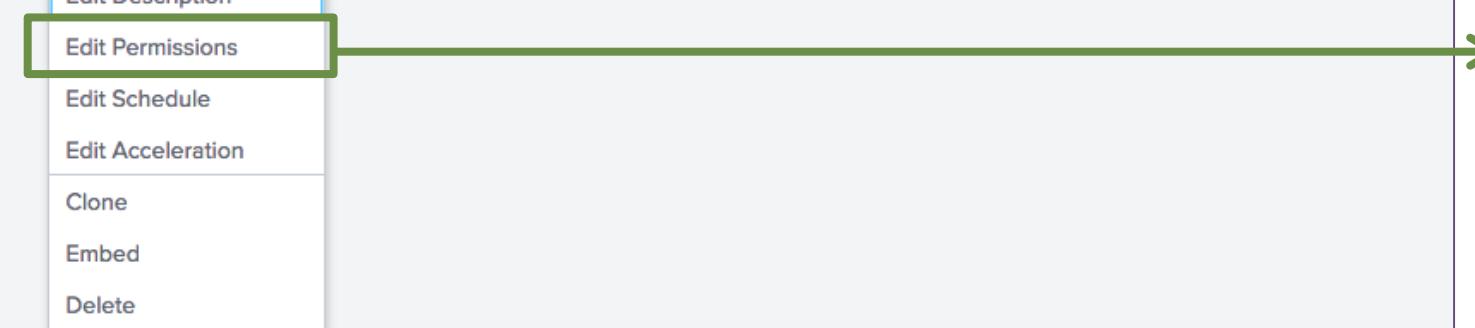
**Reports**

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.

1 Reports

|   | Title                      | Actions               | Next Scheduled Time | Owner    | App         | Sharing |
|---|----------------------------|-----------------------|---------------------|----------|-------------|---------|
| > | IT_Report_FailedRootLogins | Open in Search Edit ▾ | None                | student1 | class_Fund1 | Private |

The 'Edit' dropdown menu is open, showing options: Edit Description, Edit Permissions (highlighted with a green box), Edit Schedule, Edit Acceleration, Clone, Embed, and Delete.



Edit Permissions

Report IT\_Report\_FailedRootLogins  
Owner student1  
App class\_Fund1

Display For  Owner  App  All apps

Run As  Owner  User

Learn More ▾

|                    | Read                     | Write                    |
|--------------------|--------------------------|--------------------------|
| Everyone           | <input type="checkbox"/> | <input type="checkbox"/> |
| admin              | <input type="checkbox"/> | <input type="checkbox"/> |
| can_delete         | <input type="checkbox"/> | <input type="checkbox"/> |
| power              | <input type="checkbox"/> | <input type="checkbox"/> |
| splunk-system-role | <input type="checkbox"/> | <input type="checkbox"/> |
| student            | <input type="checkbox"/> | <input type="checkbox"/> |
| user               | <input type="checkbox"/> | <input type="checkbox"/> |
| windows-admin      | <input type="checkbox"/> | <input type="checkbox"/> |

Cancel Save

Generated for () (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 following sequence of screenshots illustrates the process of enabling report embedding:

- Screenshot 1: Reports Page**

Shows the 'Reports' section with a search bar and filter options. A single report titled 'IT\_Report\_FailedRootLogins' is listed.
- Screenshot 2: Edit Menu**

The 'Edit' dropdown menu for the report is open, showing options like 'Edit Description', 'Edit Permissions', 'Edit Schedule', 'Edit Acceleration', 'Clone', and 'Embed'. The 'Embed' option is highlighted with a green box and an arrow pointing to the next step.
- Screenshot 3: Enable Report Embedding Dialog**

A modal dialog titled 'Enable Report Embedding' asks if the user is sure they want to enable embedding for the report. It explains that an embedded report can be viewed by anyone with access to the web page(s) in which it is inserted. The 'Enable Embedding' button is highlighted with a green box and an arrow pointing to the final step.
- Screenshot 4: Embed Configuration Dialog**

The 'Embed' configuration dialog displays a warning about the report not having data until the scheduled search runs. It contains a code snippet for an iframe and a 'Done' button.

Generated for () (C) Splunk Inc, not for distribution

# What Are Alerts?

---

- 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:
  - Create an entry in Triggered Alerts
  - Log an event
  - Output results to a lookup file
  - Send emails
  - Use a webhook
  - Perform a custom action

Generated for () (C) Splunk Inc, not for distribution

# 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

New Search

index=web sourcetype=access\_combined status=50\*

128 events (1/9/18 9:00:00.000 PM to 1/10/18 9:48:39.000 PM) No Event Sampling

Events (128) Patterns Statistics Visualization

Note

This is the underlying search on which all the subsequent Alert slides are based.

Save As ▾ Close

- Report
- Dashboard Panel
- Alert**
- Event Type

Cancel Save

Save As Alert

Settings

Title: Web server errors

Description: Alerts when http status 50\* events are returned

Permissions: Private (selected)

Alert type: Scheduled

Trigger Conditions

Trigger alert when: Per-Result

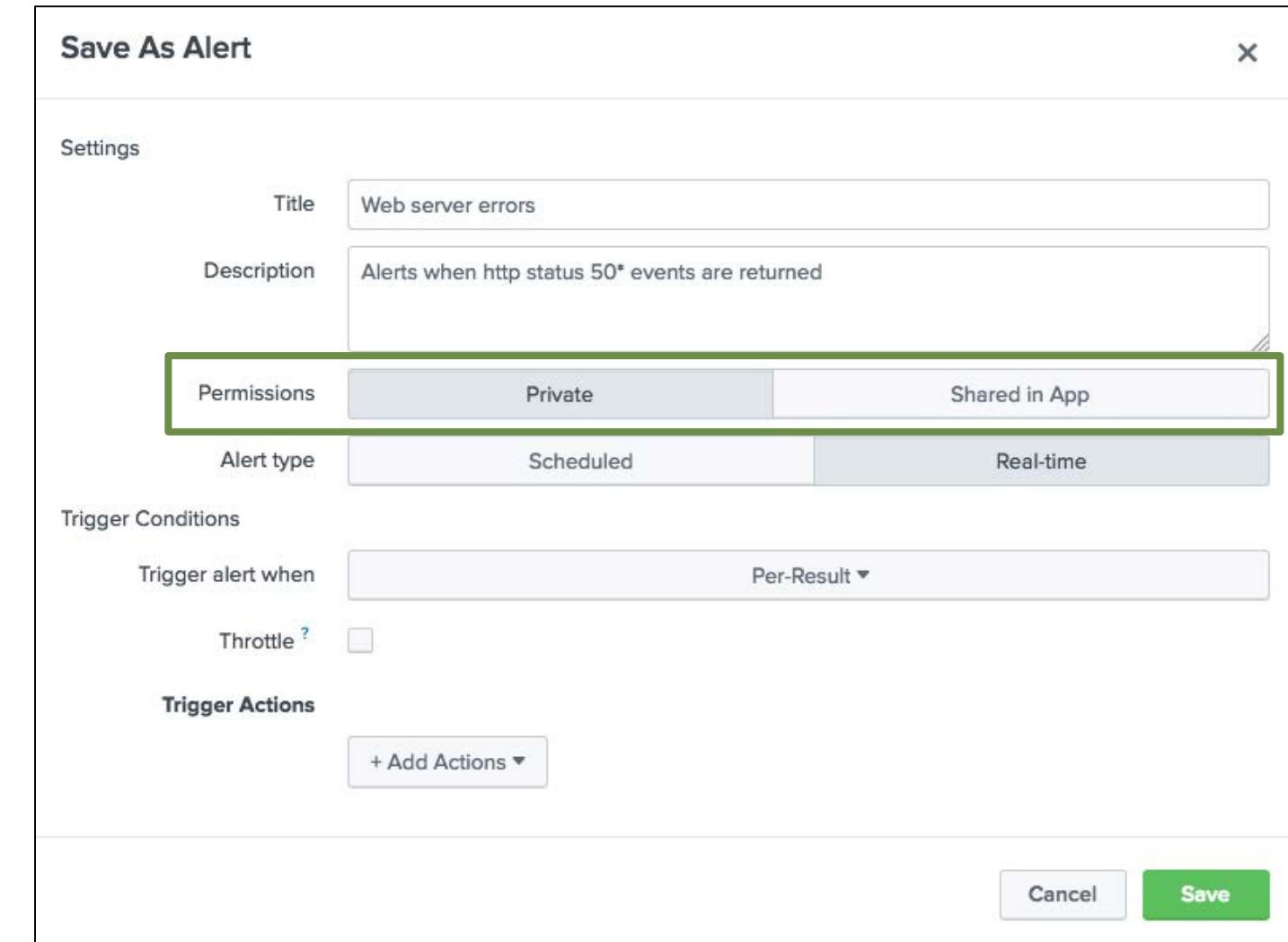
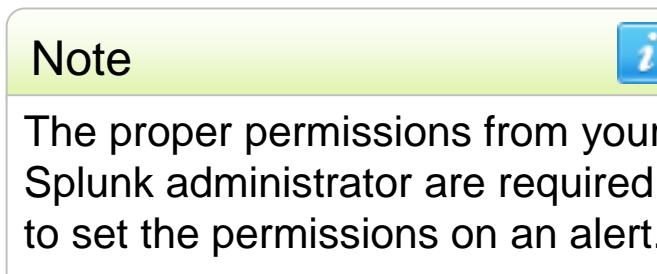
Throttle:

Trigger Actions

+ Add Actions ▾

# Setting 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



The dialog box is titled "Save As Alert". It contains fields for "Title" (Web server errors) and "Description" (Alerts when http status 50\* events are returned). A "Permissions" tab is selected, showing "Private" is chosen. Below it, an "Alert type" section shows "Scheduled" is selected. Under "Trigger Conditions", "Trigger alert when" is set to "Per-Result". There is a "Throttle" checkbox which is unchecked. In the "Trigger Actions" section, there is a "+ Add Actions" button. At the bottom right are "Cancel" and "Save" buttons.

Generated for () (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 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 ?                                  | <input type="checkbox"/>        |   |
| Trigger Actions                             | <a href="#">+ Add Actions ▾</a> |   |
| <a href="#">Cancel</a> <a href="#">Save</a> |                                 |   |

Generated for () (C) Splunk Inc, not for distribution

# 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** (highlighted)

Real-time

Time Range:

Cron Expression: 0 6 \* \* 1  
e.g. 00 18 \*\*\* (every day at 6:00 PM)

Trigger Conditions

Trigger alert when: is greater than 0

Run on Cron Schedule ▾

- Run every hour
- Run every day
- Run every week
- Run every month
- Run on Cron Schedule** (highlighted)

Cancel Save

# Setting Trigger Conditions – Scheduled

- For the cron schedule, choose a Time Range and enter a Cron Expression
- 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

Scenario ?

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

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 ▾

Time Range: Last 5 minutes ▾

Cron Expression: 0 6 \* \* 1  
e.g. 00 18 \*\*\* (every day at 6PM). Learn More

Trigger Conditions

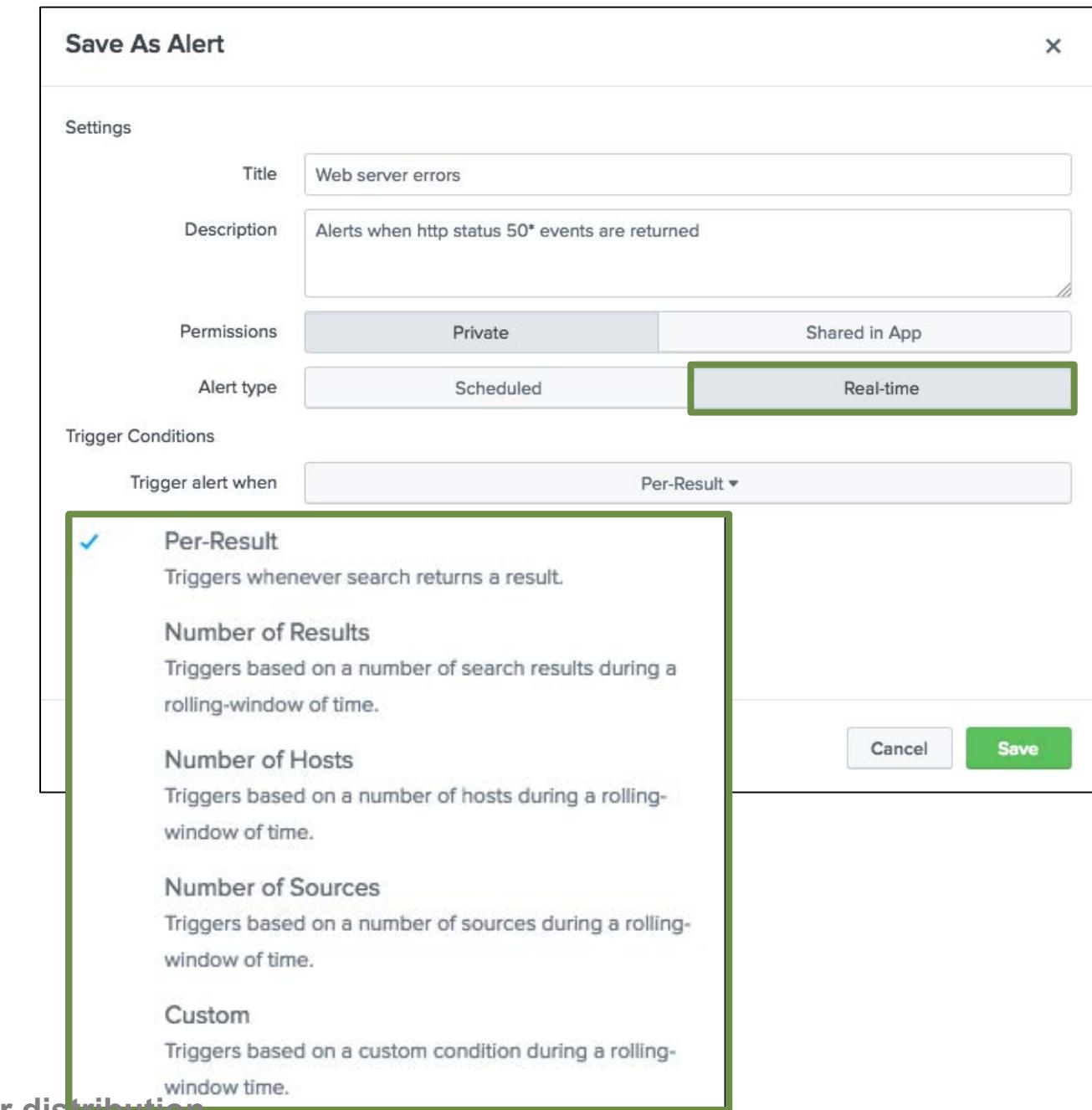
Trigger alert when: Number of Results ▾  
is greater than ▾ 2

Cancel Save

Generated for () (C) Splunk Inc, not for distribution

# Setting Trigger Conditions – Real-time

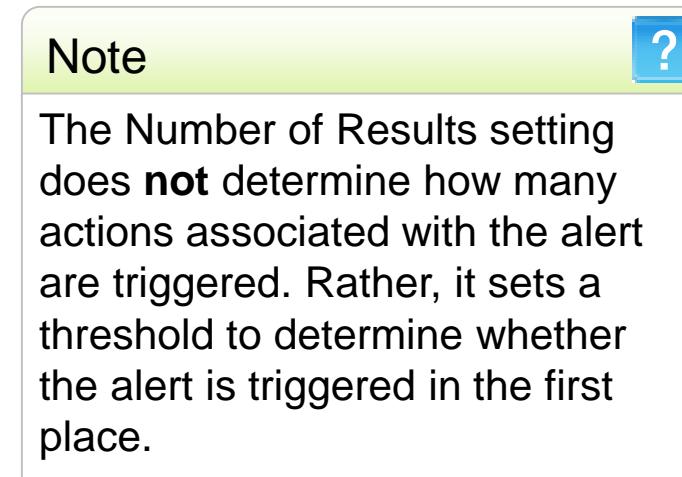
- Trigger conditions allow you to capture a larger data set, then apply more stringent criteria to results before executing the alert
- You can set alerts to trigger:
  - **Per-Result** – triggers when a result is returned
  - **Number of Results** – define how many results are returned before the alert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



Generated for () (C) Splunk Inc, not for distribution

# 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:

Trigger Actions

Cancel Save

A green box highlights the 'Trigger Conditions' section of the alert configuration.

Generated for () (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 **Throttle** option to suppress the actions for results within a specified time range

Save As Alert

Alert type: Scheduled    Real-time

Run on Cron Schedule ▾

Time Range: Last 5 minutes ▾

Cron Expression: 0 6 \* \* 1  
e.g. 00 18 \*\*\* (every day at 6PM). Learn More

Trigger Conditions

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

Trigger: Once    For each result

Throttle ?   
Suppress triggering for: 10 minute(s) ▾

Trigger Actions

+ Add Actions ▾

Cancel    Save

The screenshot shows the 'Save As Alert' dialog box. Under 'Trigger Conditions', the 'Trigger' dropdown is set to 'Once'. Below it, the 'Throttle' checkbox is checked, and the 'Suppress triggering for' field is set to 10 minutes. The entire 'Throttle' section is highlighted with a green border.

# Alert Actions – Trigger Conditions: For Each Result

- **For each result** – executes the alert actions once *for each result* that matches the conditions
- Select the Throttle 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, 20 with status=503
  - Since *For each result* is selected, **two actions** trigger—one for each status

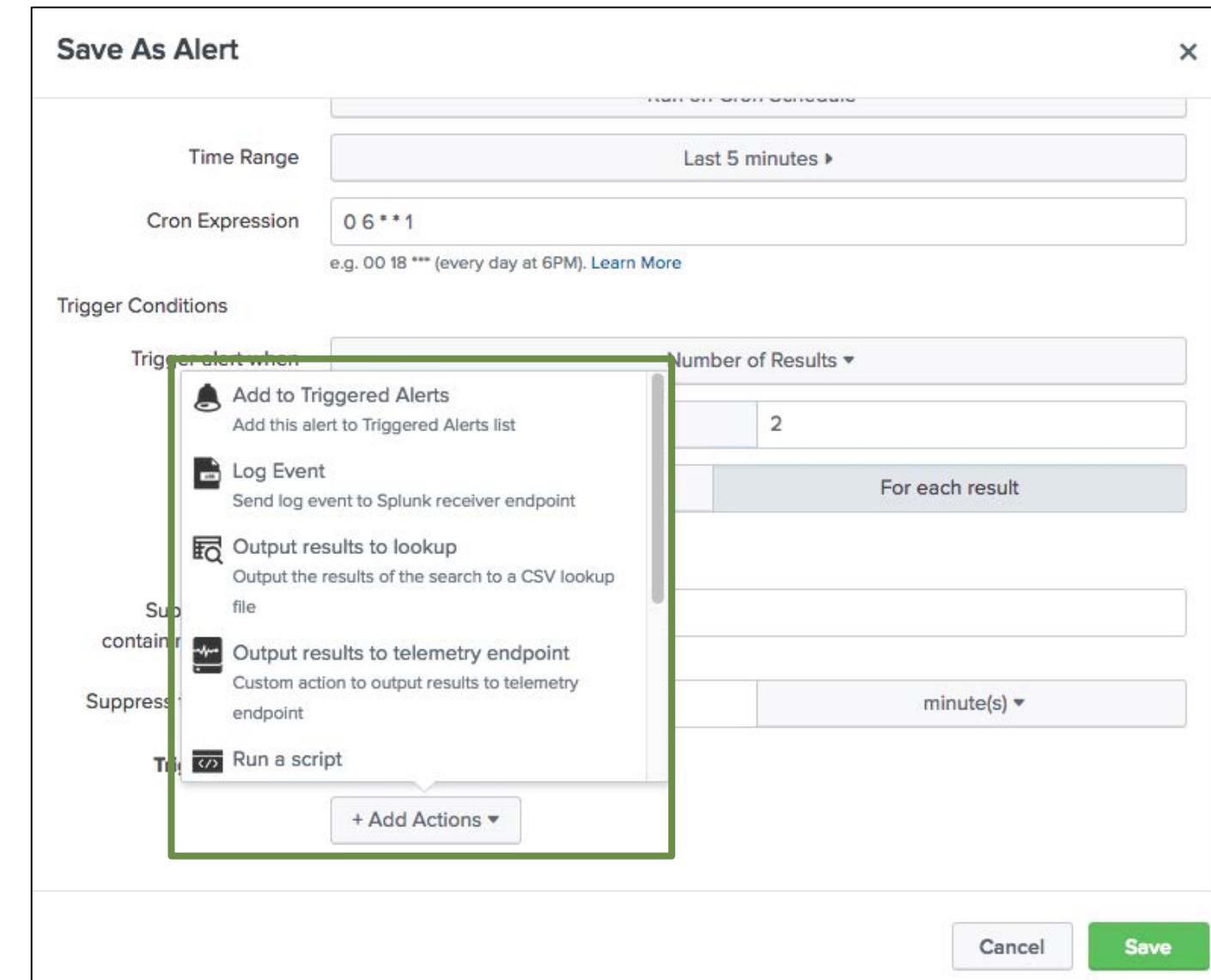
Save As Alert

|   |  |                 |
|---|--|-----------------|
| Alert type                              | Scheduled  | Real-time       |
| Run on Cron Schedule ▾                  |  |                 |
| Time Range                              | Last 5 minutes ▾   |                 |
| Cron Expression                         | 0 6 * * 1<br>e.g. 00 18 *** (every day at 6PM). <a href="#">Learn More</a> |                 |
| 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 () (C) Splunk Inc, not for distribution

# Add Trigger Actions

- Add to Triggered Alerts – adds the alert to the Activity > Triggered alerts list
- All actions available for scheduled reports are also available for alerts:
  - Log Event
  - Output results to lookup
  - Output results to telemetry endpoint
  - Run a script
  - Send email
  - Webhook



Generated for () (C) Splunk Inc, not for distribution

# Alert Actions – Add to Triggered Alerts

Choose an appropriate severity for the alert

**Save As Alert**

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

**Trigger Conditions**

Trigger alert when Number of Results ▾  
is greater than 2

Trigger Once For each result

Throttle ?

Skip results containing field value status

Skip triggering for 10 minute(s) ▾

**Trigger Actions**

+ Add Actions ▾

When triggered Add to Triggered Alerts Remove

Severity Medium ▾

- Info
- Low
- Medium
- High
- Critical

App CLASS: Fundamentals 1 (class\_Fund1) Owner student... Severity All Alert All ▾

Showing 1-12 of 12 results

| Time ▾                  | Fired alerts ▾    | App         | Type ▾    | Severity ▾ | Mode ▾ | Actions   |
|-------------------------|-------------------|-------------|-----------|------------|--------|---|
| 2018-01-11 00:26:29 UTC | Web server errors | class_Fund1 | Real-time | Medium     | Digest | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |
| 2018-01-11 00:26:28 UTC | Web server errors | class_Fund1 | Real-time | Medium     | Digest | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |
| 2018-01-11 00:26:24 UTC | Web server errors | class_Fund1 | Real-time | Medium     | Digest | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |
| 2018-01-11 00:26:23 UTC | Web server errors | class_Fund1 | Real-time | Medium     | Digest | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |
| 2018-01-11 00:26:19 UTC | Web server errors | class_Fund1 | Real-time | Medium     | Digest | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |

Generated for () (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 new log event
- **Source** – Source of the new log event (by default, the alert name)
- **Sourcetype** – Sourcetype to which the new log event will be written
- **Host** – Host field value of the new log event (by default, IP address of the host of the alert)
- **Index** – Destination index for the new log event (default value is main)

When triggered

Log Event

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 generic\_single\_line

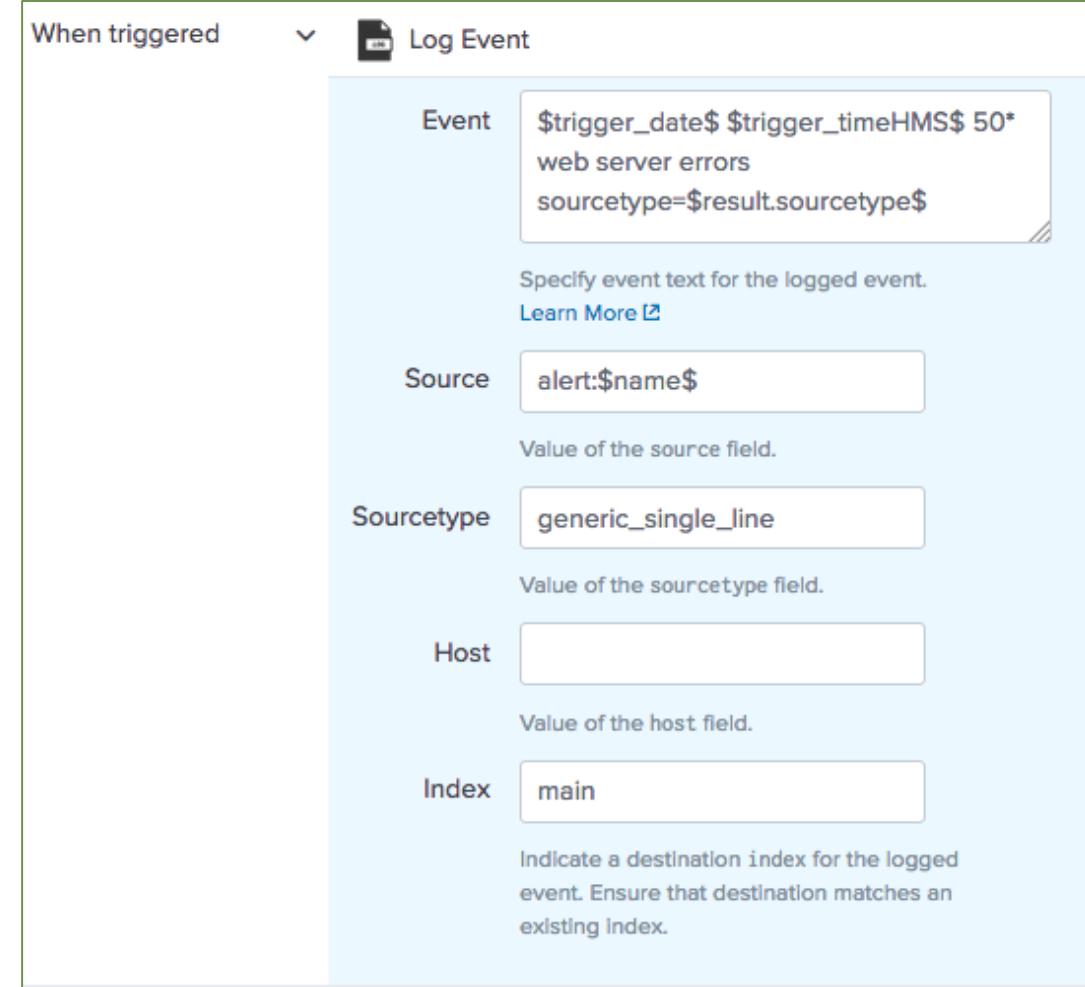
Value of the sourcetype field.

Host

Value of the host field.

Index main

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



## 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 illustrates the configuration of an alert action to log events. On the left, the 'Log Event' configuration window is shown with the following fields:

- Event:** \$trigger\_date\$ \$trigger\_timeHMS\$ 50\*  
web server errors  
sourcetype=\$result.sourcetype\$
- Source:** alert:\$name\$
- Sourcetype:** generic\_single\_line
- Host:** [empty]
- Index:** main

The 'New Search' window on the right shows the results of the search defined in the alert configuration. The search results are as follows:

| Time                   | Event  |
|------------------------|--|
| 2018-01-11 12:00:20 PM | host = 127.0.0.1   source = alert:Web server errors   sourcetype = generic_single_line |
| 2018-01-11 11:59:29 AM | host = 127.0.0.1   source = alert:Web server errors   sourcetype = generic_single_line |
| 2018-01-11 11:56:39 AM | host = 127.0.0.1   source = alert:Web server errors   sourcetype = generic_single_line |

Generated for () (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

When triggered   Send email

To   
Comma separated list of email addresses.  
[Show CC and BCC](#)

Priority

Subject

Message   
The email subject, recipients 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

Generated for () (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 Enterprise web interface. The top navigation bar includes links for 'splunk>enterprise', 'Apps', 'student1', 'Messages', 'Settings', 'Activity' (which is currently selected), and 'Help'. A search bar with a magnifying glass icon is also present. Below the navigation, there are several search filters: 'App' (set to 'CLASS: Fundamentals 1 (class\_F...)'), 'Owner' (set to 'student...'), 'Severity' (set to 'All'), and an 'Alert' dropdown menu. The 'Alert' menu is open, showing options: 'Jobs' (selected) and 'Triggered Alerts' (highlighted with a green box). Below the filters, there are buttons for '<prev' and 'next>' and a message indicating 'Showing 1-12 of 12 results'. The main content area displays a table of triggered alerts. The columns are: Time, Fired alerts, App, Type, Severity, Mode, and Actions. The table lists three entries, each corresponding to a 'Web server errors' event from 'class\_Fund1' at different times on January 11, 2018. Each row includes a checkbox, the timestamp, the fired alert type, the app name, the event type, the severity, the mode, and a set of 'Actions' buttons for 'View results', 'Edit search', and 'Delete'.

| Time                    | Fired alerts      | App         | Type      | Severity | Mode   | Actions   |
|-------------------------|-------------------|-------------|-----------|----------|--------|---|
| 2018-01-11 00:26:29 UTC | Web server errors | class_Fund1 | Real-time | Medium   | Digest | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |
| 2018-01-11 00:26:28 UTC | Web server errors | class_Fund1 | Real-time | Medium   | Digest | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |
| 2018-01-11 00:26:24 UTC | Web server errors | class_Fund1 | Real-time | Medium   | Digest | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |

Generated for () (C) Splunk Inc, not for distribution

# Editing Alerts

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

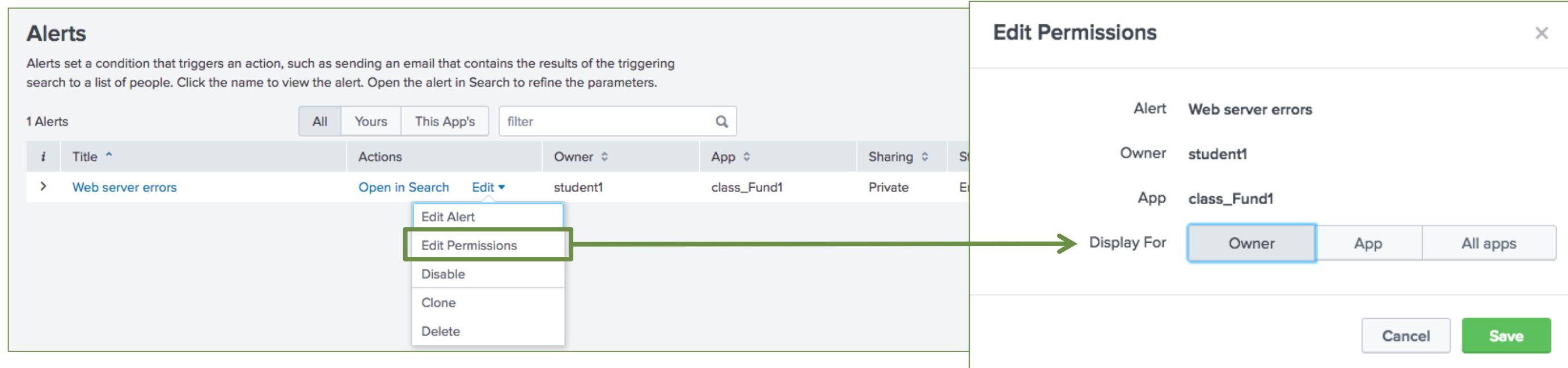
The screenshot shows the Splunk interface with the following details:

- Top Navigation Bar:** Search, Datasets, Reports, **Alerts**, Dashboards, Presentation ▾, Lab Solutions ▾, Instructor ▾, CLASS: Fundamentals 1.
- Alerts Page Header:** Alerts, Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.
- Alerts Table:** 1 Alerts. Columns include Title (sorted by title), Actions, Owner, App, Sharing, and Status.
- Action Column:** Contains links for each alert: Open in Search, Edit ▾ (with a dropdown menu), and Delete.
- Context Menu (highlighted by a green box and arrow):** Edit Alert, Edit Permissions, Disable, Clone, Delete.

Generated for () (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 () (C) Splunk Inc, not for distribution

# What's Next?: *Splunk Fundamentals 2*

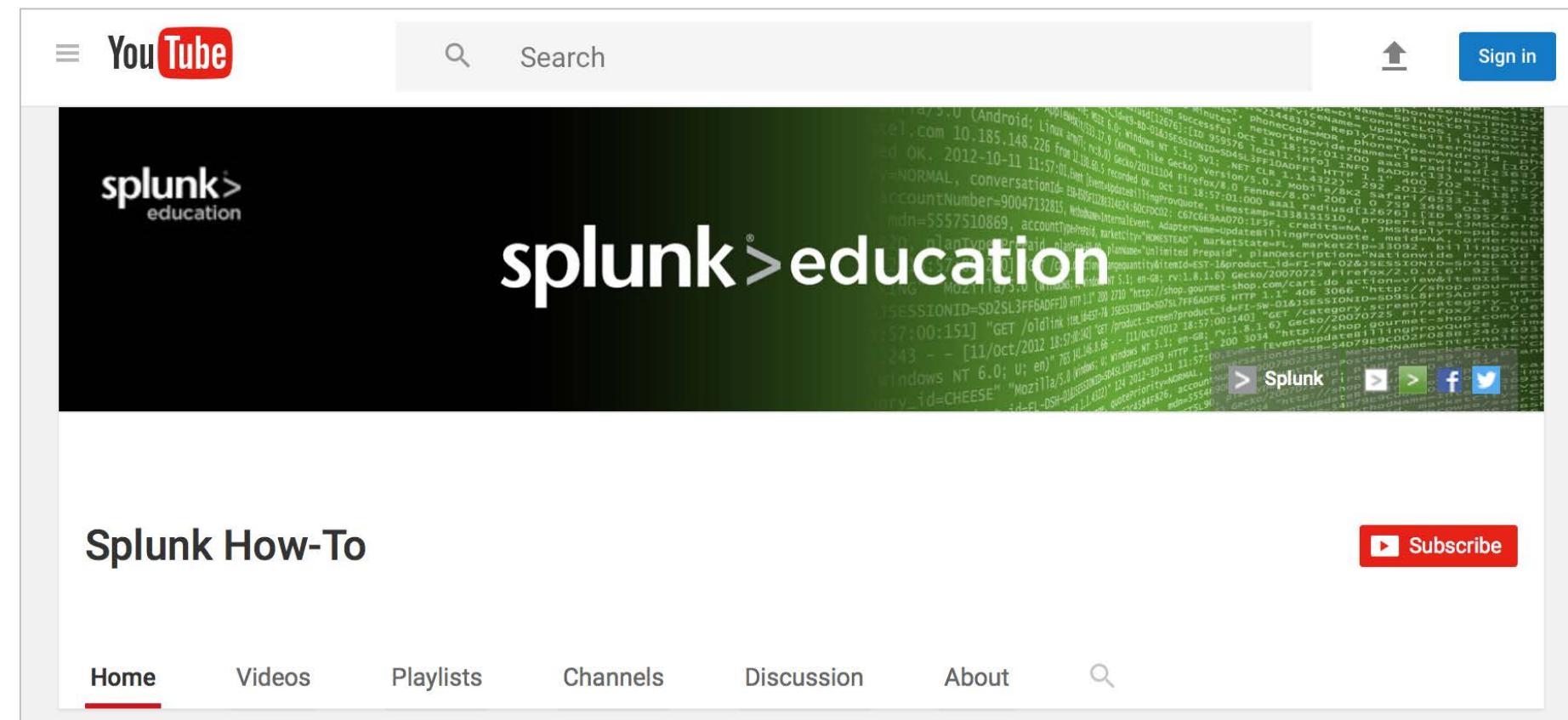
---

- Use transforming commands and visualizations
- Filter and format the results of a search
- Correlate events into transactions
- Create and manage Knowledge Objects
- Create & manage extracted fields, field aliases, calculated fields
- Create tags and event types
- Create and use macros and workflow objects
- Create and manage data models
- Use the Splunk Common Information Model (CIM)

Generated for () (C) Splunk Inc, not for distribution

# YouTube: The Splunk How-To Channel

- In addition to our roster of training courses, check out the Splunk Education How-To channel: <http://www.youtube.com/c/SplunkHowTo>
- This site provides useful, short videos on a variety of Splunk topics



Generated for () (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](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.)

Generated for () (C) Splunk Inc, not for distribution

# Other Resources

---

- Splunk App Repository  
<https://splunkbase.splunk.com/>
- Splunk Answers  
<http://answers.splunk.com/>
- Splunk Blogs  
<http://blogs.splunk.com/>
- Splunk Wiki  
<http://wiki.splunk.com/>
- Splunk Docs  
<http://docs.splunk.com/Documentation/Splunk>
- Splunk User Groups  
<http://usergroups.splunk.com/>

Generated for () (C) Splunk Inc, not for distribution