



# Creating Dashboards

# Document Usage Guidelines

---

- Should be used only by enrolled students
- Not meant to be a self-paced document, an instructor is needed
- Do not distribute

Generated for Matt Brown ([mbrown@idbny.com](mailto:mbrown@idbny.com)) (C) Splunk Inc, not for distribution

# Course Prerequisites

## Classes

- Splunk Fundamentals 1 & 2
- Splunk Fundamentals 3 (suggested)

## Skills

- Working knowledge of XML
- Experience with HTML, CSS, and JavaScript

Important



In order to receive credit for this course, you must complete all lab exercises.

# Course Goals

---

- Apply best practices when creating views
- Capture and access dynamic values
- Optimize dashboard performance
- Create well formed, global searches
- Customize dashboard appearance
- Create dynamic drilldowns and behaviors
- Troubleshoot views

# Course Outline

---

Module 1: Creating a Prototype

Module 2: Using Forms

Module 3: Improving Performance

Module 4: Customizing Dashboards

Module 5: Using Drilldowns

Module 6: Adding Advanced Behaviors & Visualizations

# Course Scenario

- As in the other Splunk courses, the use cases in this course are based on a gaming company called Buttercup Games
- The views are based on business analytics from web server logs and lookups



Data	Host	Sourcetype	Interesting Fields
Online transactions & web server	www1	access_combined	action, bytes, categoryId, clientip, itemId, JSESSIONID, price, productId, product_name, referer, referer_domain, sale_price, status, user, useragent
	www2		
	www3		
Retail sales data	vendorUS1	vendor_sales	AcctID, categoryId, product_name, productId, sale_price, Vendor, VendorCity, VendorCountry, VendorID, VendorStateProvince
Server access data	www1	linux_secure	action, app, dest, process, src_ip, src_port, user, vendor_action
	www2		
	www3		
	mailsv1		

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# 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



How can we link multiple views to investigate data from different perspectives?

## Notes & Tips

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

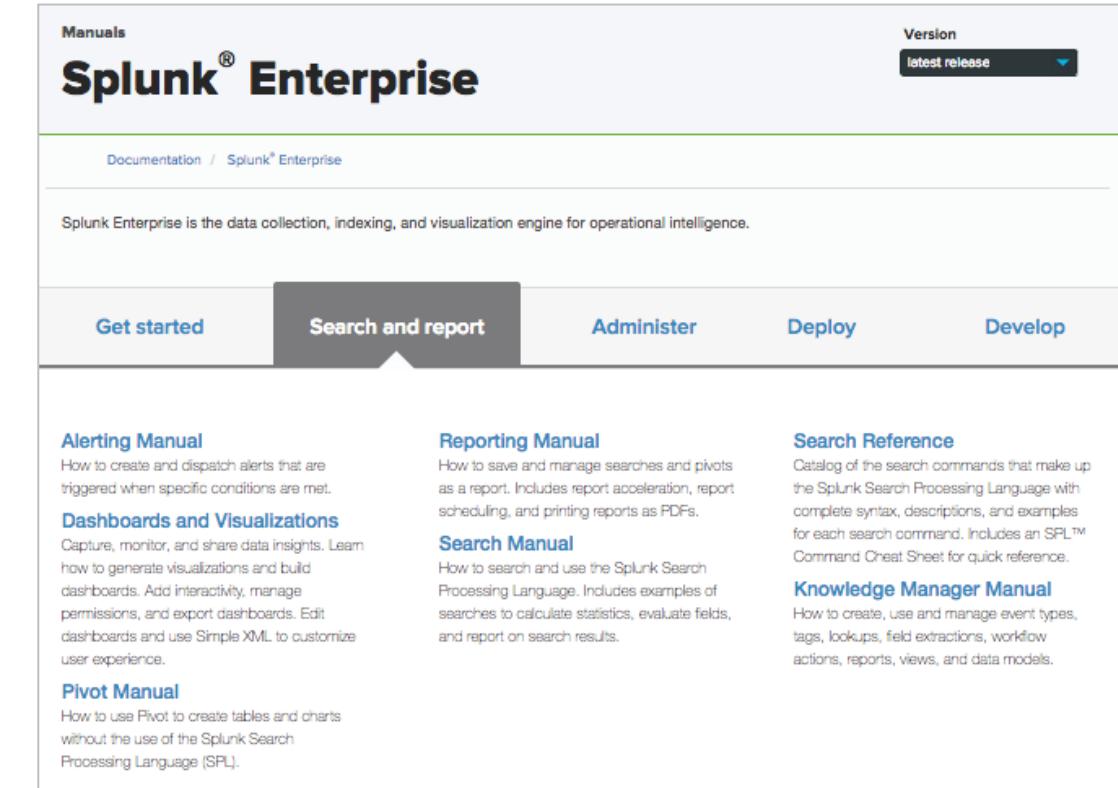
### Note



Functions and arguments used with stats and chart can also be used with timechart.

# Useful References

- Dashboards & Visualizations Manual:  
[docs.splunk.com/Documentation/Splunk/latest/Viz](https://docs.splunk.com/Documentation/Splunk/latest/Viz)
- Dashboards Quick Reference:  
[splunk.com/pdfs/solution-guides/splunk-dashboards-quick-reference-guide.pdf](https://splunk.com/pdfs/solution-guides/splunk-dashboards-quick-reference-guide.pdf)
- Search Quick Reference:  
[splunk.com/content/dam/splunk2/pdfs/solution-guides/splunk-quick-reference-guide.pdf](https://splunk.com/content/dam/splunk2/pdfs/solution-guides/splunk-quick-reference-guide.pdf)
- Reporting Manual:  
[docs.splunk.com/Documentation/Splunk/latest/Report/Createandeditreports](https://docs.splunk.com/Documentation/Splunk/latest/Report/Createandeditreports)
- Knowledge Manager Manual:  
[docs.splunk.com/Documentation/Splunk/latest/Knowledge/WhatisSplunkknowledge](https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/WhatisSplunkknowledge)



The screenshot shows the Splunk Enterprise Documentation homepage. At the top right, there is a "Version" dropdown set to "latest release". The main title is "Splunk® Enterprise" with a "Manuals" link above it. Below the title, there is a breadcrumb navigation: "Documentation / Splunk® Enterprise". A brief description states: "Splunk Enterprise is the data collection, indexing, and visualization engine for operational intelligence." Below the description is a horizontal navigation bar with five tabs: "Get started" (blue), "Search and report" (dark grey, selected), "Administer" (blue), "Deploy" (blue), and "Develop" (blue). To the right of the navigation bar, there are four columns of documentation links:

- Alerting Manual**: How to create and dispatch alerts that are triggered when specific conditions are met.
- Dashboards and Visualizations**: Capture, monitor, and share data insights. Learn how to generate visualizations and build dashboards. Add interactivity, manage permissions, and export dashboards. Edit dashboards and use Simple XML to customize user experience.
- Pivot Manual**: How to use Pivot to create tables and charts without the use of the Splunk Search Processing Language (SPL).
- Reporting Manual**: How to save and manage searches and pivots as a report. Includes report acceleration, report scheduling, and printing reports as PDFs.
- Search Manual**: How to search and use the Splunk Search Processing Language. Includes examples of searches to calculate statistics, evaluate fields, and report on search results.
- Search Reference**: Catalog of the search commands that make up the Splunk Search Processing Language with complete syntax, descriptions, and examples for each search command. Includes an SPL™ Command Cheat Sheet for quick reference.
- Knowledge Manager Manual**: How to create, use and manage event types, tags, lookups, field extractions, workflow actions, reports, views, and data models.

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Module 1: Creating a Prototype

Generated for Matt Brown ([mbrown@idbny.com](mailto:mbrown@idbny.com)) (C) Splunk Inc, not for distribution

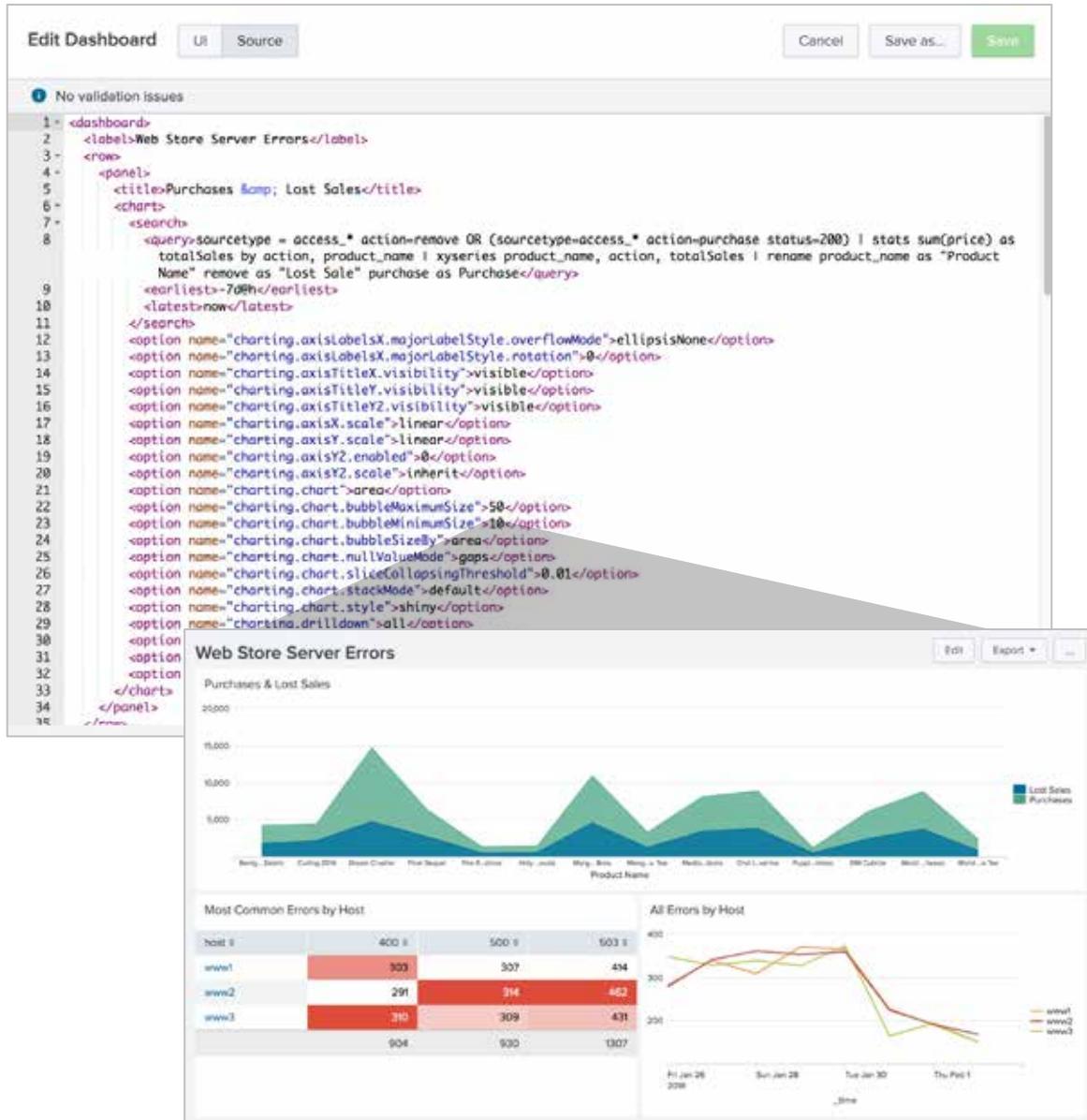
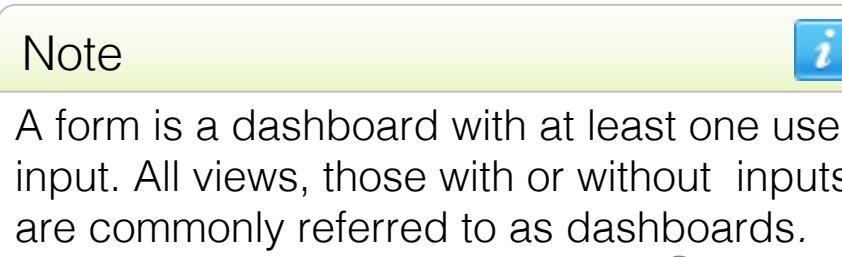
# Module Objectives

---

- Name the components of a view
- Compare dashboard and form simple XML syntax
- Troubleshoot views
- Use best practices for creating views
- Identify the primary transforming commands

# What is a view?

- Every page in Splunk Web is a view
  - Dashboards
  - Forms
- Each view is a web page built from:
  - Simple XML file that defines the content
  - HTML file that defines the layout
  - CSS and JavaScript files that define the appearance and interactions



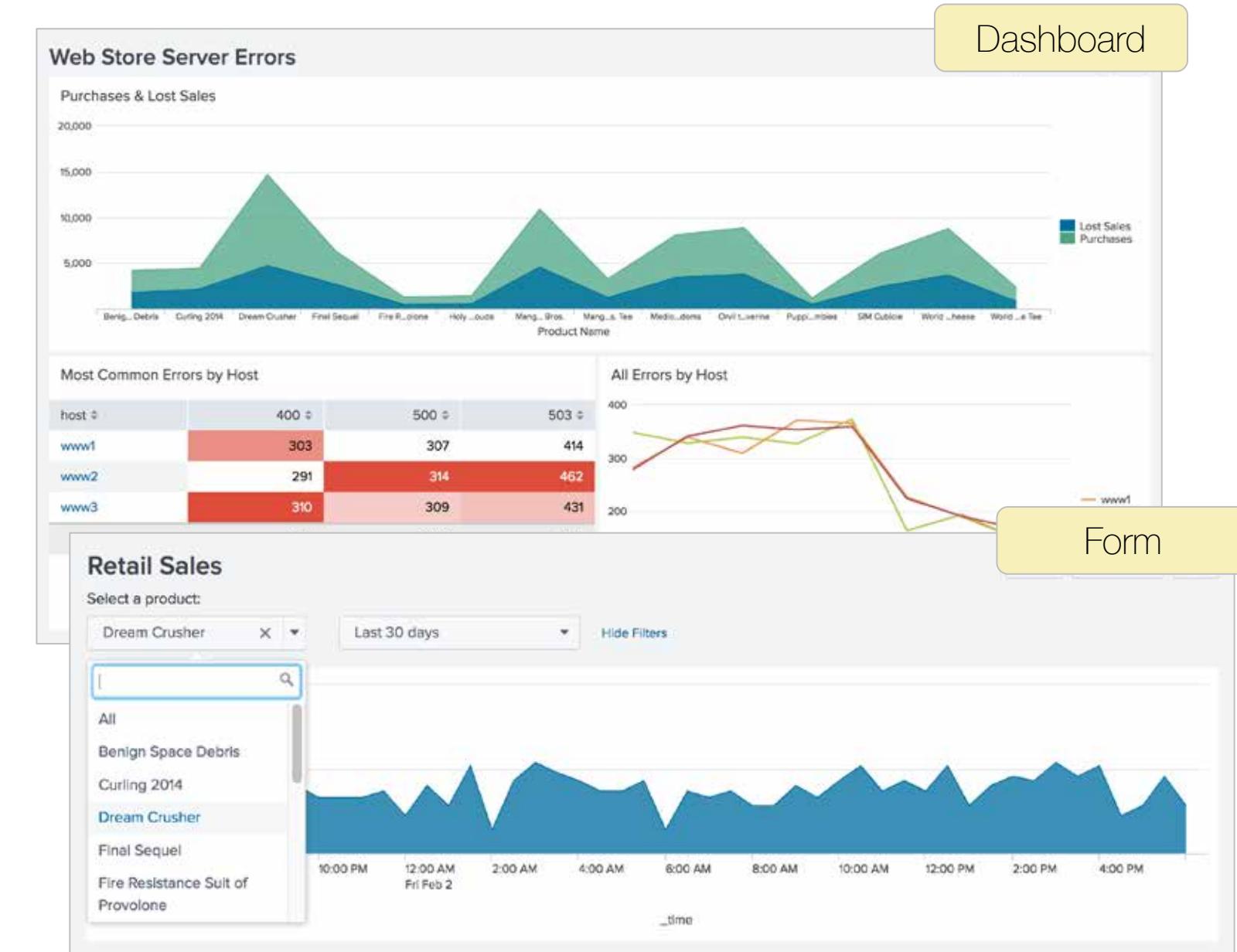
# Dashboards & Forms

- Dashboard

- Most common type of view
- Limited user input
- Default interactive features

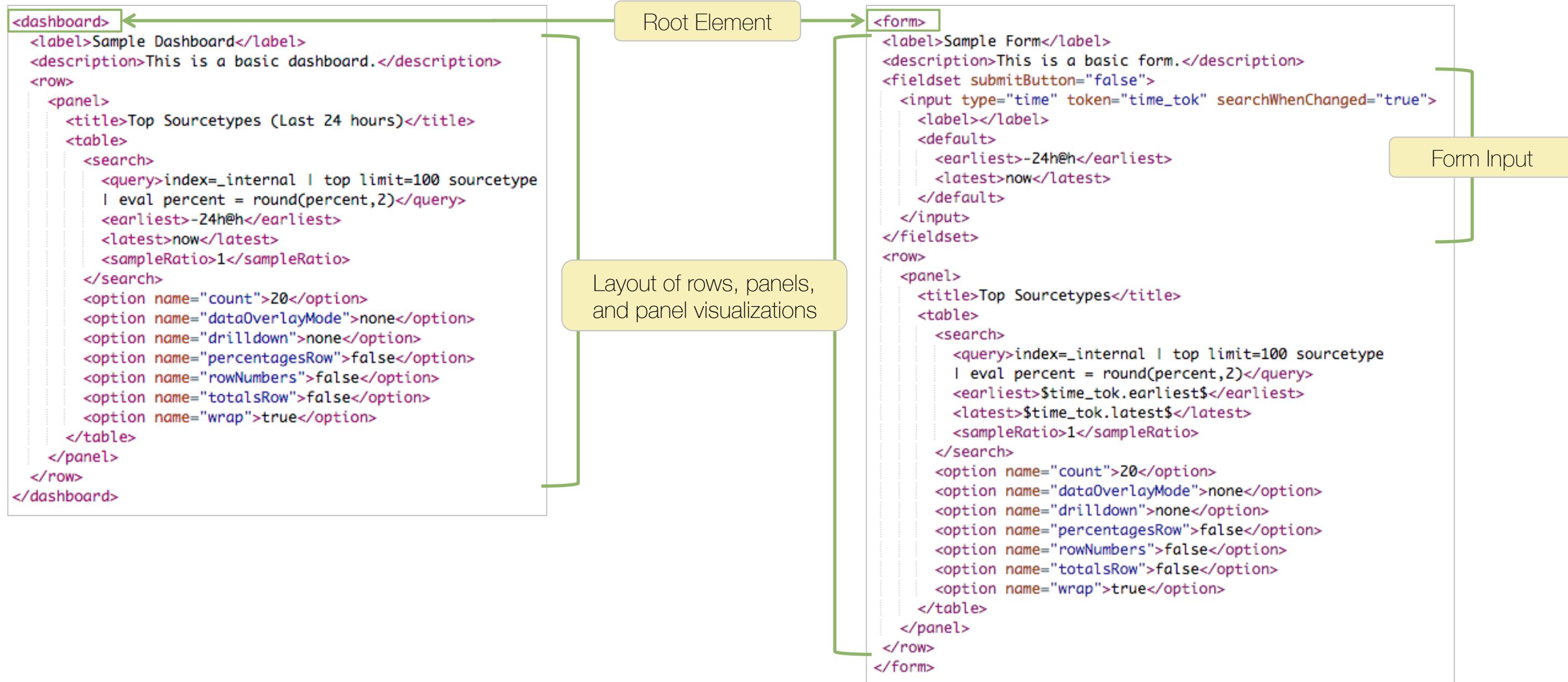
- Form

- Enter values from a variety of inputs
- User input stored as tokens



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

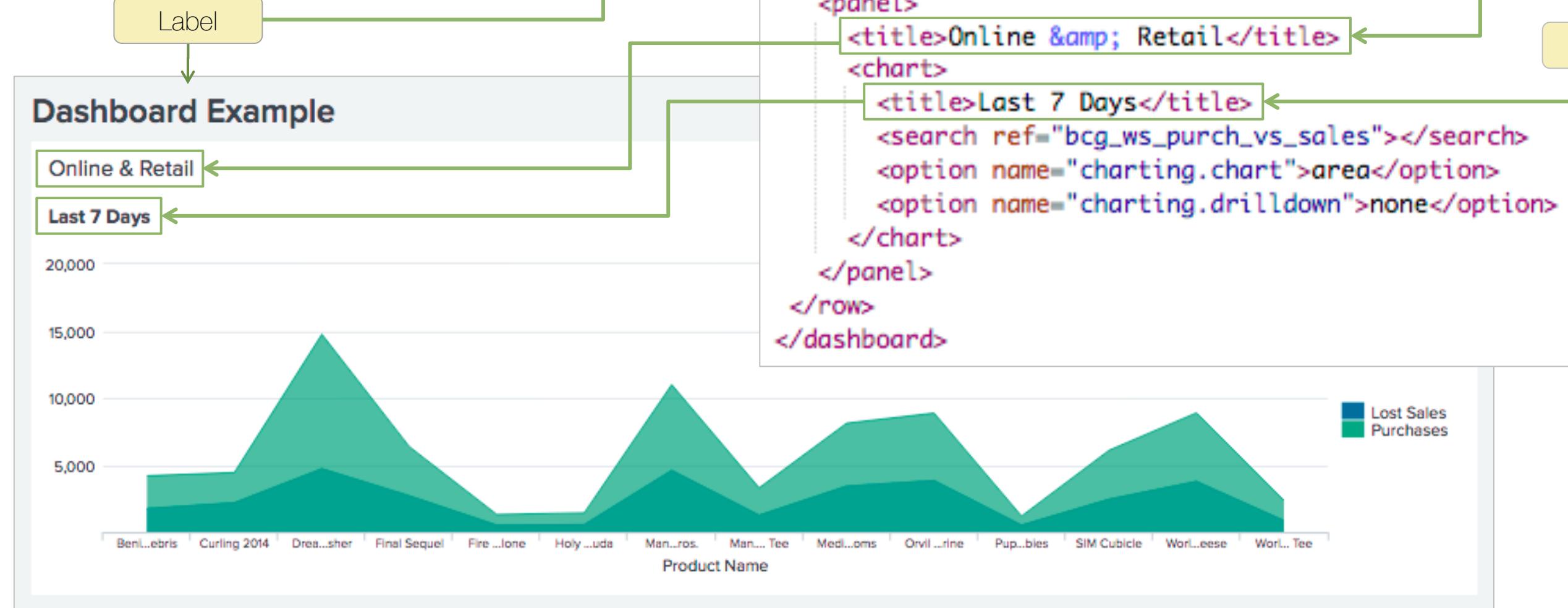
# Dashboards & Forms – (cont.)



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

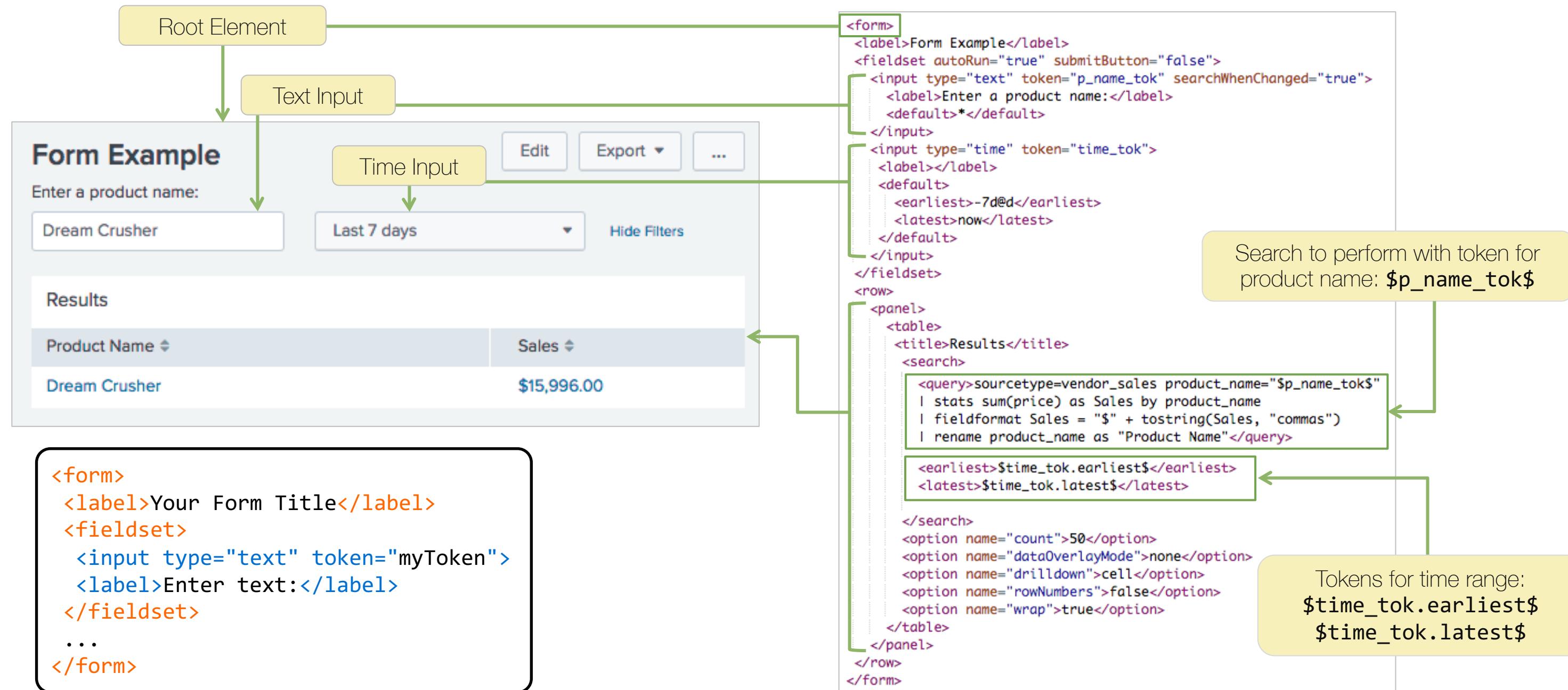
# Simple XML Syntax – Dashboard

```
<dashboard>
  <label>Your Dashboard Title</label>
  ...
</dashboard>
```



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Simple XML Syntax – Form



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# XML Source Editor

The screenshot shows the XML Source Editor interface with several features highlighted:

- Inline Validation:** A yellow callout points to the validation messages on the left side of the code editor.
- Auto Indent & Outdent:** A yellow callout points to the code editor area showing auto-indentation.
- Code Folding:** A yellow callout points to the collapsed sections of the XML code.
- Theme:** A yellow callout points to the theme setting in the top navigation bar.
- Search & Replace (can use regex):** A yellow callout points to the search and replace dialog.
- Line Wrapping:** A yellow callout points to the line wrapping settings in the search and replace dialog.
- Save changes as new dashboard:** A yellow callout points to the "Save" button in the top right corner.
- Exit without saving:** A yellow callout points to the "Cancel", "Save as...", and "Save" buttons in the top right corner.

The XML code in the editor is as follows:

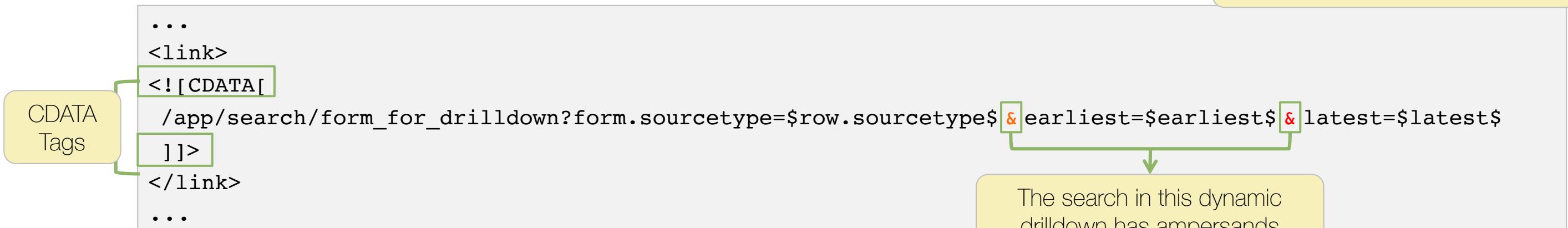
```
<dashboard theme="light">
    <label>XML Source Editor</label>
    <row>
        <panel>
            <title>Purchases & Lost Sales</title>
            <chart>
                <searchString>
                    |> query(index=sales sourcetype=access_combined (action=remove OR action=purchase) | stats sum(price) as totalSales by action,
                    |> xyseries product_name, action, totalSales | rename product_name as "Product Name", remove as "Lost Sales"
                    |> purchases
                </searchString>
                <option name="charting.chart">column</option>
                <option name="charting.chart.nullValueMode">gaps</option>
                <option name="charting.chart.sliceCollapsingThreshold">0.01</option>
                <option name="charting.chart.stackMode">stacked</option>
                <option name="charting.chart.style">shiny</option>
                <option name="charting.legend.labelStyle.overflowMode">ellipsisMiddle</option>
                <option name="charting.legend.mode">standard</option>
                <option name="charting.legend.placement">bottom</option>
                <option name="charting.lineWidth">2</option>
            </chart>
        </panel>
    </row>
    <row><!--></row>
    <row><!--></row>
</dashboard>
```

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Escaping Special Characters

- Some characters have special meaning in an XML file and cannot be used literally
- Wrap any text with special characters within CDATA tags

```
<![CDATA[ "Text within tags" ]]>
```



Character	Replacement Entity
"	&quot;
'	&apos;
<	&lt;
>	&gt;
&	&amp;

```
...  
<condition match="$job.resultCount$ >= 5 ">  
  <set token="result_count_condition">Matched!</set>  
</condition>  
...
```

This conditional match statement uses the greater than (>) entity.

The search in this dynamic drilldown has ampersands

# Troubleshooting Views

- Examine the view's source
  - Check for search and XML syntax errors
  - Run search manually
- View all previous searches
  - Examine your search history
  - Run `| history`
- Expand macros and event types
- Verify the tokens are being set and have the expected values
  - Create an html panel that shows all your tokens
  - Use the **View what tokens are available** dashboard in the Splunk Dashboard Examples app

The screenshot shows the Splunk user interface. On the left, there is a sidebar with the title "Search History". Below it is a table with three rows of search history entries. The columns are labeled "Search", "Actions", and "Last Run". The first entry is "Search". The second entry is "sourcetype=access\_combined (action=remove OR action=pu...)" with "Add to Search" and "2 hours ago". The third entry is "lstats summariesonly=t count from datamodel='bcg\_ws\_xl' ... with "Add to Search" and "4 hours ago". At the top right of the interface, there is a search results panel titled "Retail Purchases" which displays the message "Search did not return any events."

Search	Actions	Last Run
Search		
sourcetype=access_combined (action=remove OR action=pu...)	Add to Search	2 hours ago
lstats summariesonly=t count from datamodel='bcg_ws_xl' ...	Add to Search	4 hours ago

Generated for Matt Brown ([mbrown@idbny.com](mailto:mbrown@idbny.com)) (C) Splunk Inc, not for distribution

# Troubleshooting Views (cont.)

- Job Inspector
  - Examine impact of knowledge object processing, such as event types, tags, lookups etc.

The screenshot shows the 'Jobs' view in Splunk. A context menu is open over a selected job entry. The menu items shown are 'Edit Job Settings...', 'Extend Job Expiration', and 'Inspect Job'. A green box highlights the 'Jobs' tab in the top navigation bar, and a green arrow points from this box down to the 'Inspect Job' option in the context menu.

- Search Job Inspector
  - Debug messages

## Search job inspector

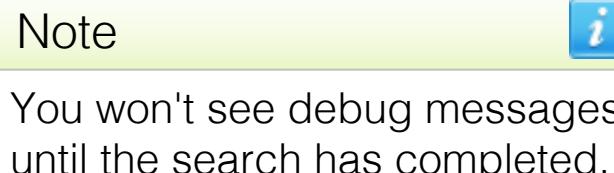
This search has completed and has returned **96** results by scanning **0** events in **0.02** seconds

(SID: admin\_\_admin\_\_advdash\_\_search6\_1519675197.116) [search.log](#)

> Execution costs

> Search job properties

Server info: Splunk 7.1.0, 52.12.249.252, Mon Feb 26 12:46:02 2018 User: admin



# Managing Views

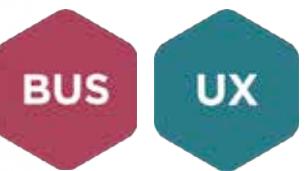
Views are scoped to your app context and permissions can be applied to them

The image shows a composite screenshot of a Splunk interface. On the left, a navigation sidebar is open under the 'User interface' section. Step 1 highlights the 'User interface' link. Step 2 highlights the 'Views' link within the 'User interface' section. On the right, the 'Views' management page is displayed. Step 3 highlights the 'App' dropdown menu set to 'Search & Reporting (s...)'. Step 4 highlights the 'Sharing' column header, which is outlined in green. The table lists 29 items, each with columns for View name, Owner, App, Sharing (with options like Global or App), Status, and Actions (Clone, Open). The first few rows include '\_admin', 'alert', 'alerts', 'charting', 'dashboard', and 'dashboard\_live'.

View name	Owner	App	Sharing	Status	Actions
_admin	No owner	system	Global   Permissions	Enabled	Clone
alert	No owner	search	Global   Permissions	Enabled	Open   Clone
alerts	No owner	search	Global   Permissions	Enabled	Open   Clone
charting	No owner	search	Global   Permissions	Enabled	Open   Clone
dashboard	No owner	search	App   Permissions	Enabled	Open   Clone
dashboard_live	No owner	search	App   Permissions	Enabled	Open   Clone
dashboards	No owner	search	Global   Permissions	Enabled	Open   Clone
data_model_editor	No owner	search	Global   Permissions	Enabled	Open   Clone
data_model_explorer	No owner	search	Global   Permissions	Enabled	Open   Clone
data_model_manager	No owner	search	Global   Permissions	Enabled	Open   Clone

Generated for Matt Brown (mbrown@dbny.com) (C) Splunk Inc, not for distribution

# Panels



## Panel Example

Panel - Title

Visualization Title

1,000

500

Fri Apr 12  
2019

Sat Apr 13

Sun Apr 14

Mon Apr 15

Tue Apr 16

Wed Apr 17

Thu

\_time

```
<dashboard>
  <label>Panel Example</label>
  <row>
    <panel>
      <title>Panel - Title</title>
      <chart>
        <title>Visualization Title</title>
        <search>
          <query>sourcetype=access_combined
            | timechart count by categoryId usenull=f</query>
          <earliest>-7d@d</earliest>
          <latest>now</latest>
          <sampleRatio>1</sampleRatio>
        </search>
      </chart>
    </panel>
  </row>
</dashboard>
```

```
<panel>
  <title>
    <chart> | <event> | <html> | <map> | <single> | <table> | <viz>
  <title>
  <search>
  . . .
```

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Panels (cont.)



- HTML Panels
  - Add inline text
  - Reference text or image files
  - Reference a file from another app
  - Use HTML elements: <h1>, <h2>, <h3>, <div>, <img>, <p>, etc.

HTML File

```
<html src="myFile.html"> </html>
```

HTML file from another app

```
<html src="myApp:myFile.html"> </html>
```

Image File

```
<html>  </img> </html>
```

HTML Visualization - Example

Edit Export ...

Panel Title

Visualization Title

Hello World! This is an example of an html panel.

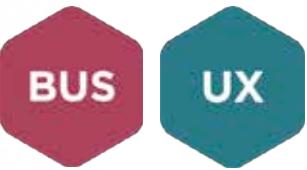
Inline Text Example

```
<dashboard>
<label>HTML Visualization - Example</label>
<row>
<panel>
<title>Panel Title</title>
<html>
<h2>Visualization Title</h2>
<p>Hello World! This is an example of an html panel.</p>
</html>
</panel>
</row>
</dashboard>
```

Note

The ability to upload files is restricted to Splunk Administrators or user roles given that right by the administrator.

# Panel Visualization Elements



Each panel has seven possible visualization elements

Element	Syntax	Description
1. Chart	<chart>	Search results as a chart, filler, marker and radial gauges
2. Event	<event>	Search results as individual events
3. Map	<map>	Search results as map
4. Single value	<single>	Single value visualizations
5. Table	<table>	Displays search results as a table
6. Custom Visualization	<viz>	Displays a Splunk Custom Visualization
7. HTML	<html>	Inline HTML. Create or edit in XML editor only

Generated for Matt Brown ([mbrown@idbny.com](mailto:mbrown@idbny.com)) (C) Splunk Inc, not for distribution

# Panel Types



- Inline
- Report
- Prebuilt

```
<dashboard>
  <label>Total Online Purchases</label>
  <row>
    <panel>
      <title>Total Online Purchases</title>
      <single>
        <search>
          <query>sourcetype=access* action=purchase status=200
            | stats count as purchases</query>
          <earliest>-30d@d</earliest>
          <latest>now</latest>
          <sampleRatio>1</sampleRatio>
        </search>
        <option name="drilldown">none</option>
      </single>
    </panel>
  </row>
</dashboard>
```

Inline Panel

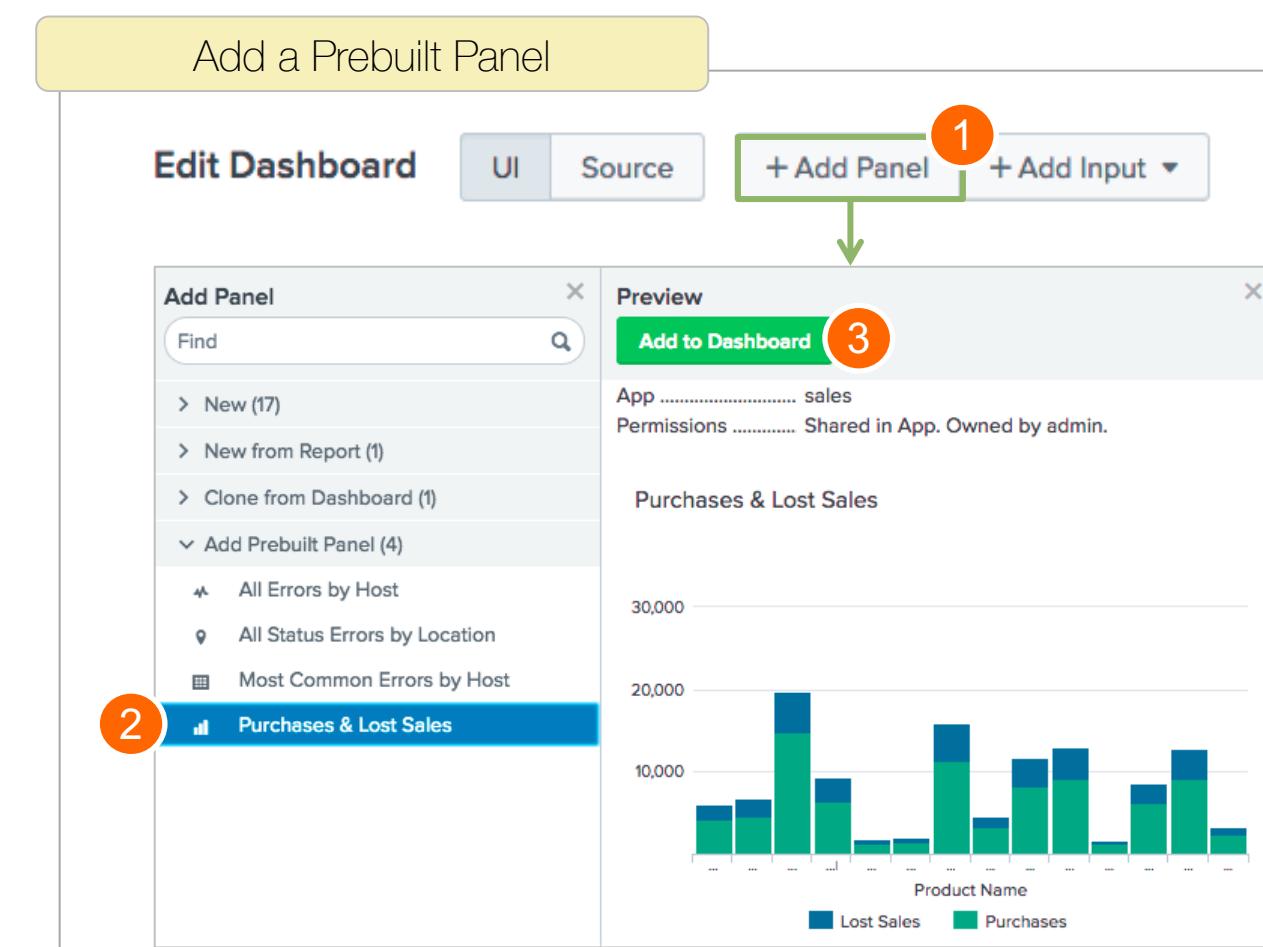
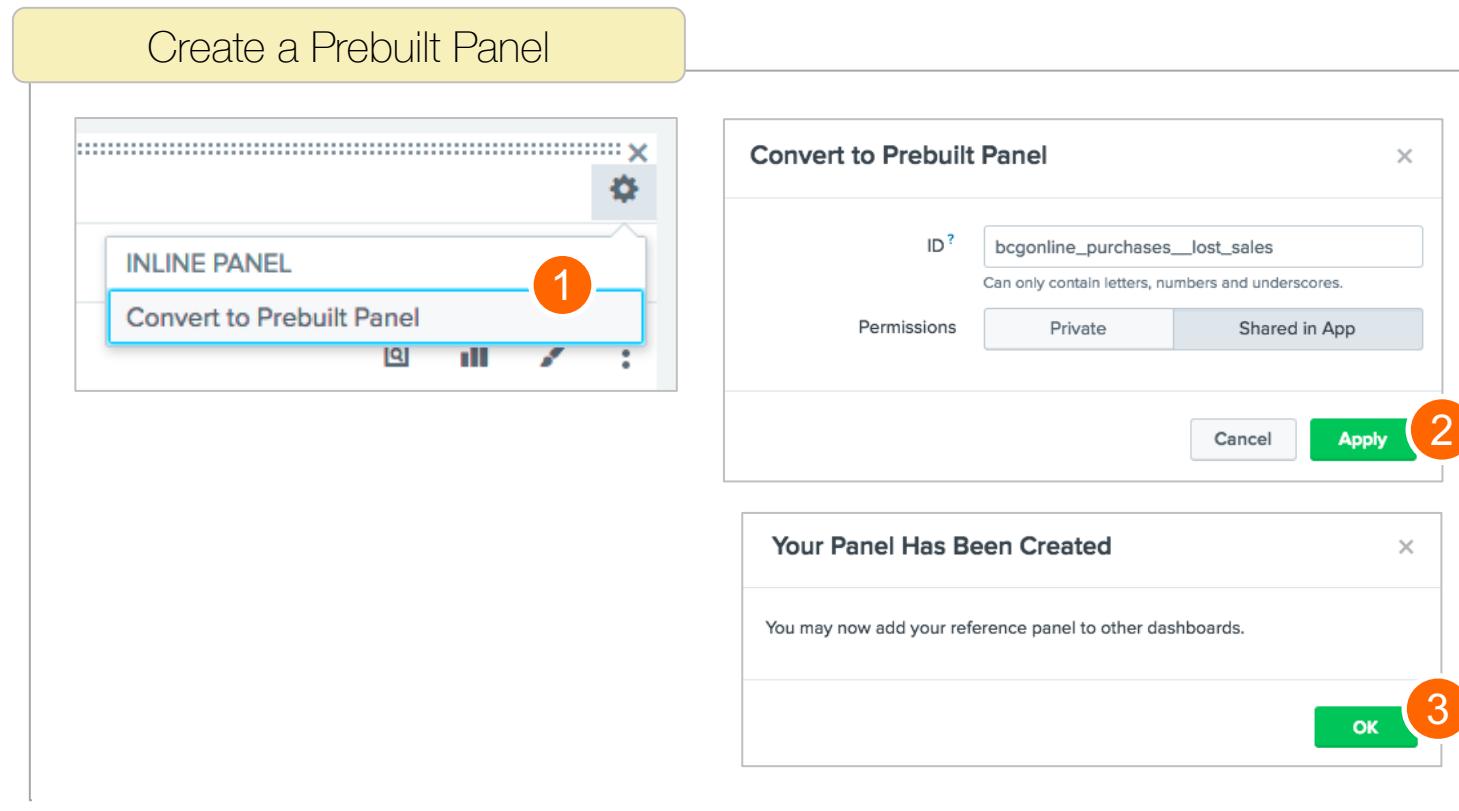
```
<dashboard>
  <label>Total Online Purchases</label>
  <row>
    <panel>
      <title>Total Online Purchases</title>
      <single>
        <search ref="Total Online Purchases"></search>
        <option name="drilldown">none</option>
      </single>
    </panel>
  </row>
</dashboard>
```

Report Panel

```
<dashboard>
  <label>Total Online Purchases</label>
  <row>
    <panel ref="total_online_purchases"></panel>
  </row>
</dashboard>
```

Prebuilt Panel

# Prebuilt Panels



- One panel, multiple dashboards
- Complex panels available to non-technical users
- All instances referencing a panel receive updates

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

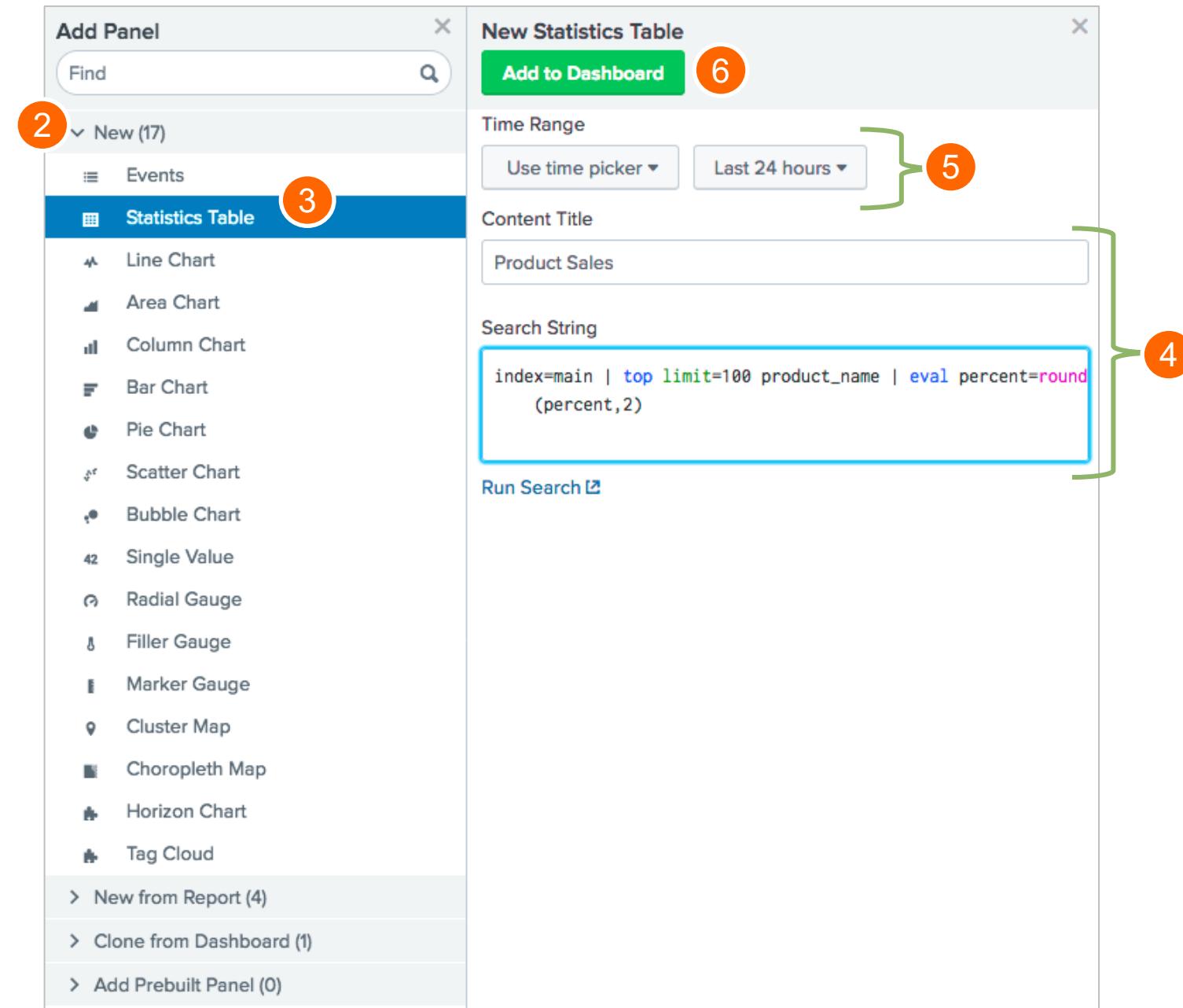
# Adding Panels

Edit Dashboard

UI    Source

+ Add Panel 1    + Add Input ▾

- Add Panel sidebar
  - New
  - New from Report
  - Clone from Dashboard
  - Add Prebuilt Panel
- Time Range
  - Use Time Picker
  - Tokens
  - Global



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Managing Prebuilt Panels

The screenshot illustrates the steps to manage prebuilt panels in the Splunk User Interface:

- Step 1:** In the left sidebar under the **KNOWLEDGE** section, the **User interface** link is highlighted with a green box and an orange circle containing the number 1.
- Step 2:** After clicking **User interface**, the main dashboard shows the **Prebuilt panels** section. The **Prebuilt panels** link is highlighted with a green box and an orange circle containing the number 2.

The main dashboard displays the following information:

- User interface**: Create and edit views, dashboards, and navigation menus.
- Time ranges**: + Add new
- Views**
- View PDF scheduling**
- Navigation menus**
- Prebuilt panels**: A green button labeled "New Prebuilt panel".
- 4 Prebuilt panels** listed in a table:

Name	Actions	Owner	App	Sharing	Status
bconline_all_errors_by_host	Add to dashboard Edit	poweruser	sales	Global	✓ Enabled
bconline_all_status_errors_by_location	Add to dashboard Edit	poweruser	sales	Global	✓ Enabled
bconline_most_common_errors_by_host	Add to dashboard Edit	poweruser	sales	Global	✓ Enabled
bconline_purchases_lost_sales	Add to dashboard Edit	poweruser	sales	Global	✓ Enabled

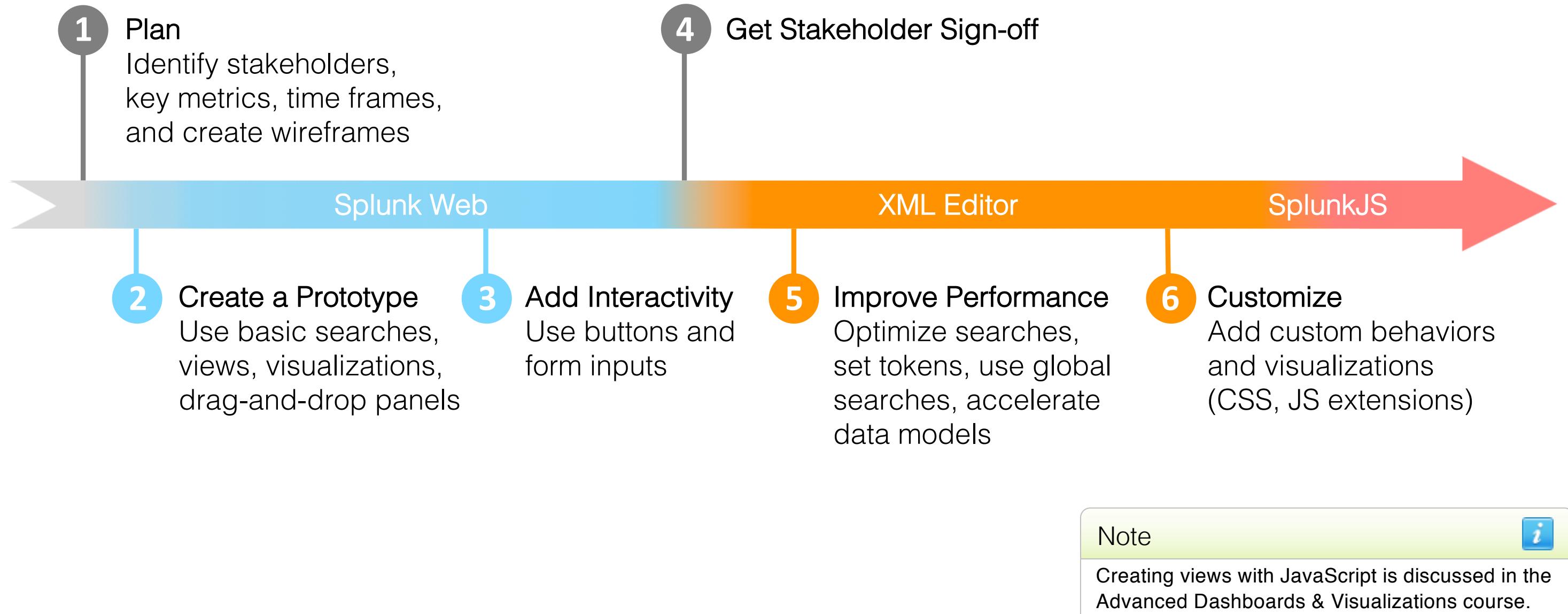
Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# What do you want to do?

	Create or modify basic dashboards	Add advanced features, optimizations, and logic	Add custom stylesheets and logic
Use this:	Dashboard Editor	Simple XML	Simple XML Extensions
Skills	Mouse click	XML	<ul style="list-style-type: none"><li>• XML</li><li>• CSS</li><li>• HTML</li><li>• JavaScript</li></ul>
Benefits	<ul style="list-style-type: none"><li>• Drag-and-drop UI</li><li>• PDF generation</li></ul>	<ul style="list-style-type: none"><li>• Complex interactivity</li><li>• More efficient dashboards</li><li>• Visualization and panel customizations</li></ul>	<ul style="list-style-type: none"><li>• Third-party libraries</li><li>• Custom behaviors</li><li>• Custom graphics</li><li>• Custom layouts</li></ul>
Drawbacks	<ul style="list-style-type: none"><li>• Limited layout</li><li>• Limited features</li></ul>	<ul style="list-style-type: none"><li>• Limited layout</li><li>• Limited features</li></ul>	None
See this:	Modules 1, 2	Modules 3, 4, 5	Module 6

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

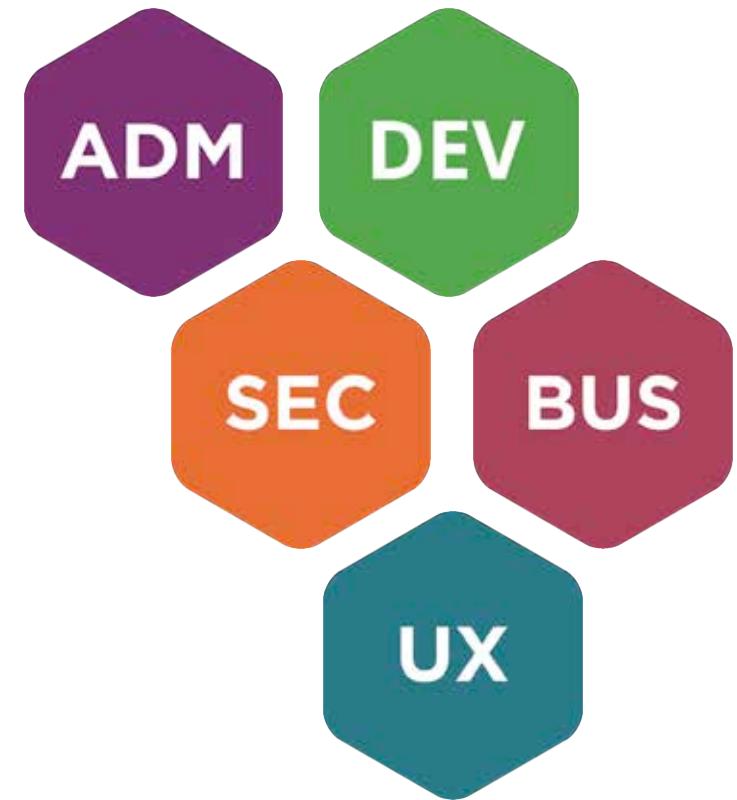
# Best Practice



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Stakeholders

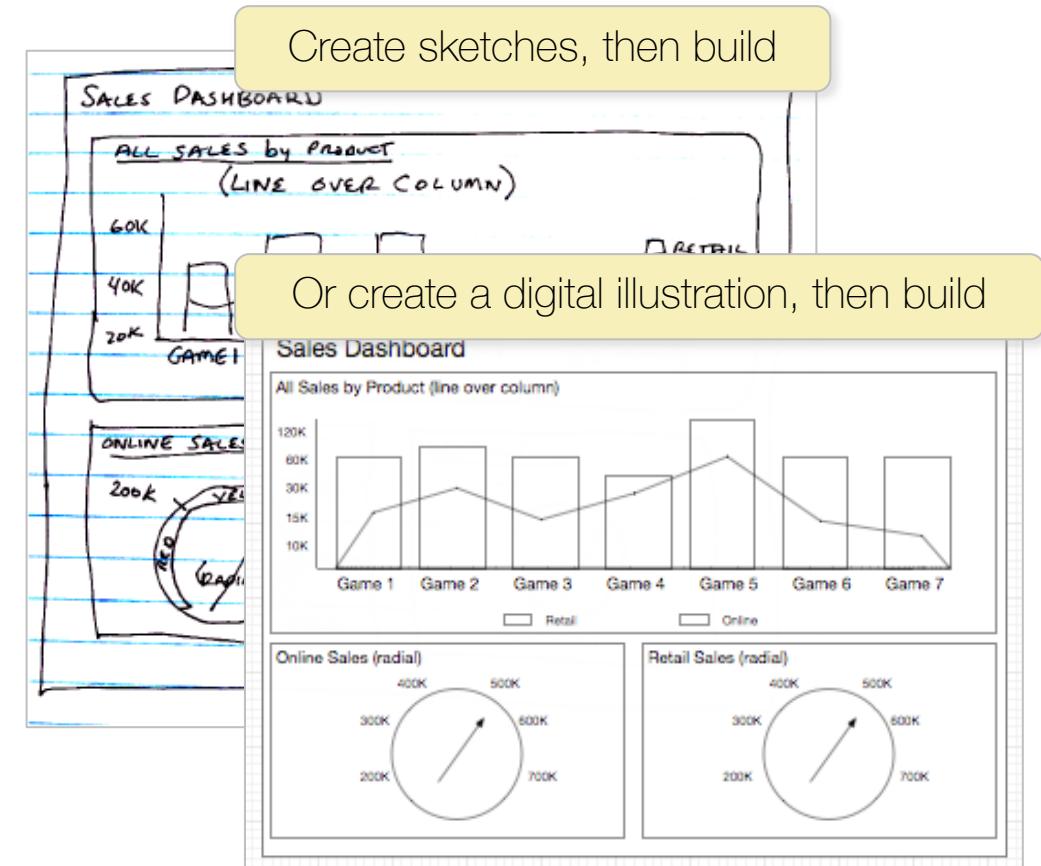
- Depending on the complexities of the view, your stakeholders may include:
  - Splunk Administrator
  - JavaScript developer
  - Security expert
  - Business user
  - UX designer
- Questions to ask:
  - How will users access your view?
  - Will the view use JavaScript or a custom stylesheet?
  - Should the view be deployed with its own app?



# Plan



- An iterative process between you and the stakeholders
  - What **critical metrics** do users want?
  - What is the **time span** for the data?
  - What is the **timeframe** for refreshing data?
  - What **visualizations** will be required?
  - What should the **layout** look like?
- Wireframing is the process of designing a view including its information, navigation, and interface design



# Create Basic Searches

- Start with basic inline searches
- Add reports, tokens, macros, and data models later
  - Use naming conventions
    - At least the same prefix
    - Group, search type, view type, platform, category, time interval, description, and project

Command	Description
bucket	Puts continuous numerical values into discrete sets.
chart	Returns results in a tabular output for charting.
dedup	Removes subsequent results that match a specified criteria.
eval	Calculates an expression and puts the value into a field.
fields	Adds or removes fields from search results.
lookup	Explicitly invokes field value lookups.
multikv	Extracts field-values from table-formatted events.
rangemap	Sets range field to the name of the ranges that match.
rex	Specify a Perl regular expression named groups to extract fields while you search.
spath	Extracts key-value pairs from XML or JSON formats.
stats	Provides statistics, grouped optionally by fields.
timechart	Create a time series chart and corresponding table of statistics.
top	Calculate a count and percentage for the most common values of the fields in the field list.
transaction	Groups search results into transactions.
where	Performs arbitrary filtering on your data.

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Transforming Commands

- Orders the results into a data table
- Transforms specified cell values into numerical values that can be used for statistical purposes
- Primary transforming commands include:
  - chart
  - timechart
  - top
  - rare
  - stats

Note

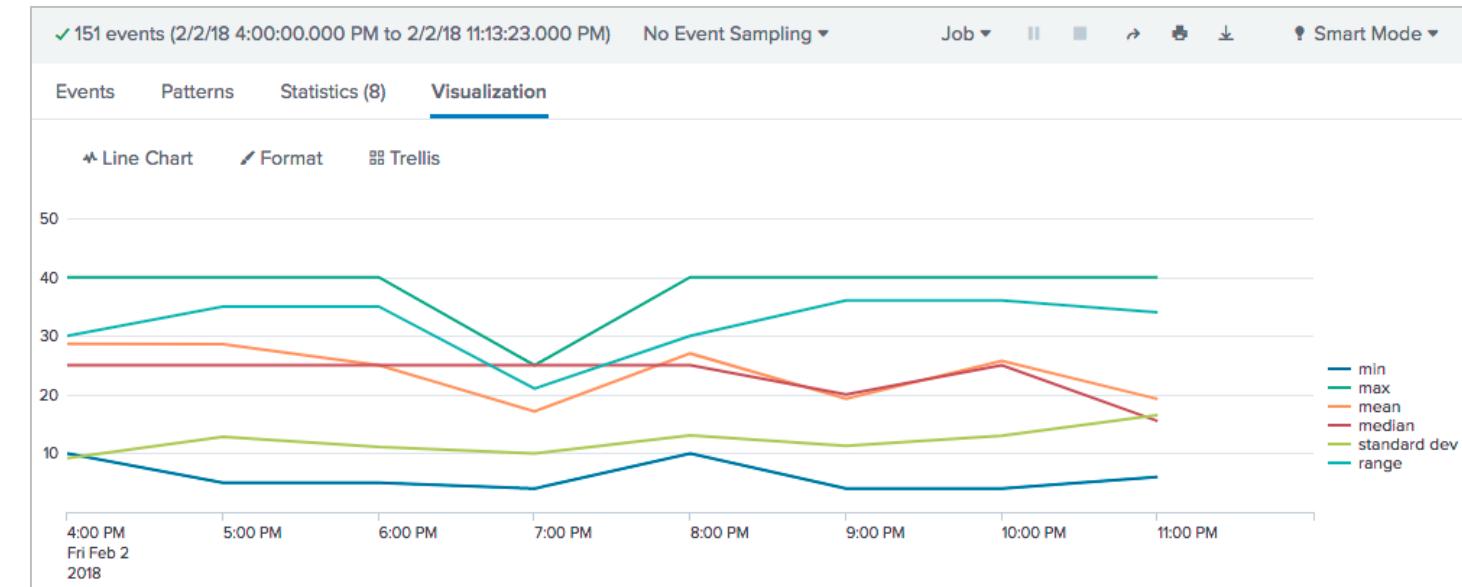


In previous versions of Splunk, transforming commands were referred to as *reporting* commands.

# Statistical Functions

- These transforming commands work with statistical functions:
  - chart, timechart, stats, geostats
- Available statistical functions:
  - count, distinct count
  - first occurrence, last occurrence
  - mean, median, mode
  - min, max, range, percentiles
  - standard deviation, variance
  - sum

```
sourcetype=access_combined action=purchase  
| timechart span=1h  
min(price) as min,  
max(price) as max,  
mean(price) as mean,  
median(price) as median,  
stdev(price) as "standard dev",  
range(price) as range
```



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Useful References

- Data Structure Requirements for Visualizations

[docs.splunk.com/Documentation/Splunk/latest/Viz/Datastructurerequirementsforvisualizations](https://docs.splunk.com/Documentation/Splunk/latest/Viz/Datastructurerequirementsforvisualizations)

- Visualization Reference

[docs.splunk.com/Documentation/Splunk/latest/Viz/Visualizationreference](https://docs.splunk.com/Documentation/Splunk/latest/Viz/Visualizationreference)

- Transforming Commands

[docs.splunk.com/Documentation/Splunk/latest/SearchReference/Commandsbytype#Transformingcommands](https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Commandsbytype#Transformingcommands)

- Statistical and Charting Functions

[docs.splunk.com/Documentation/Splunk/latest/SearchReference/CommonStatsFunctions](https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/CommonStatsFunctions)

The screenshot shows the Splunk Enterprise Documentation website. At the top right, there is a "Version" dropdown set to "Latest release". The main title is "Splunk® Enterprise" with a "Manuals" link above it. Below the title, there's a sub-navigation bar with links for "Documentation", "Splunk® Enterprise", "Splunk Enterprise is the data collection, indexing, and visualization engine for operational intelligence.", and "Get started", "Search and report" (which is highlighted in dark grey), "Administer", "Deploy", and "Develop". On the left, there's a sidebar with links for "Alerting Manual", "Reporting Manual", "Metrics", "Dashboards and Visualizations", "Search Manual", "Knowledge Manager Manual", and "Search Reference". The "Search Reference" section is expanded, showing a catalog of search commands with syntax, descriptions, and examples for each.

# Lab 1 – Create a Prototype

Time: 30 minutes

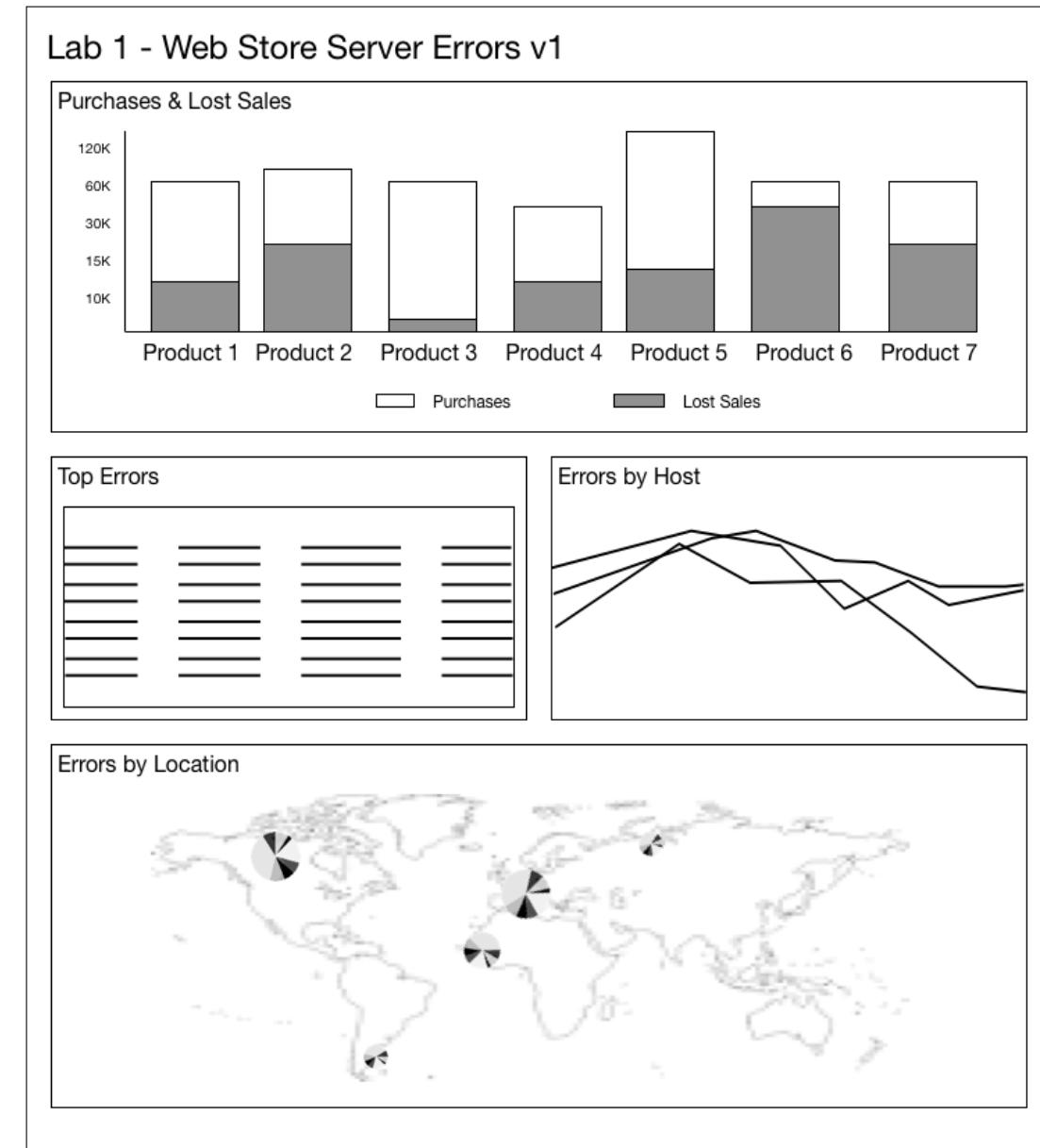
Scenario: The sales team wants a dashboard that displays information about web store server health

Tasks:

- Change the account name and time zone
- Create a dashboard
- Add table and chart panels
- Add a map
- Create prebuilt panels

Challenge Task (optional):

- Create a data model



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Module 2: Using Forms

Generated for Matt Brown ([mbrown@idbny.com](mailto:mbrown@idbny.com)) (C) Splunk Inc, not for distribution

# Module Objectives

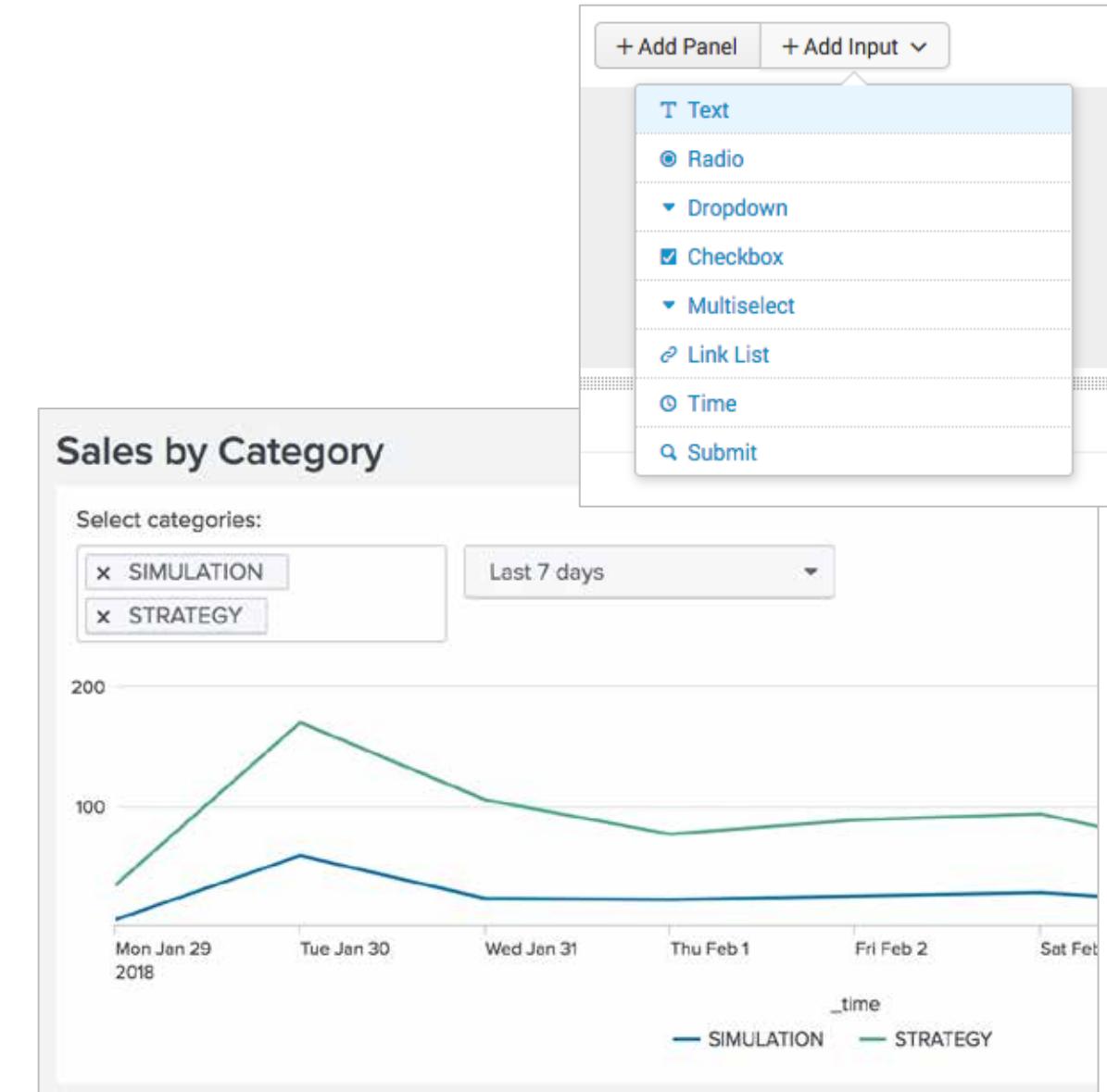
---

- Identify types of form inputs
- Describe how tokens are created and used
- Use tokens with form inputs
- Create cascading inputs
- Define types of token filters

# Form Inputs



- Adding an input changes the root element from <dashboard> to <form>
- Add to a page or panel
- User defined token for selected value
- Configure when input values populate a form:
  - On page load
  - Input change
  - Clicking Submit
- Specify default and initial values



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Tokens



- Dynamically capture and pass values
  - Form input values
  - Search terms
  - Field values
- Dashboard behavior
  - Show & Hide Panels
  - Drilldowns
  - Event handlers
  - Conditional behaviors
- User defined tokens
- Predefined tokens

```
...
<fieldset submitButton="false" autoRun="false">
  <input type="dropdown" token="prod_name_tok" searchWhenChanged="true">
    <label>Select a product:</label>
    <choice value="*">>All</choice>
    <search>
      <query>sourcetype=vendor_sales | stats count by product_name</query>
      <earliest>-7d@h</earliest>
      <latest>now</latest>
    </search>
    <default>*</default>
    <fieldForLabel>product_name</fieldForLabel>
    <fieldForValue>product_name</fieldForValue>
    <initialValue>*</initialValue>
  </input>
</fieldset>
<row>
  <panel>
    <chart>
      <title>$prod_name_tok$ Sales by City</title>
      <search>
        <query>sourcetype=vendor_sales product_name=$prod_name Tok|s$ | stats count by VendorCity, Vendor | sort - count</query>
        <earliest>-7d@h</earliest>
        <latest>now</latest>
      </search>
    ...
  ...

```

The diagram illustrates the usage of a user-defined token 'prod\_name\_tok'. It shows the token being defined in the input field's attributes, used in the chart title, and utilized in the chart's search query.

# Time Input – Example 1

The diagram illustrates the configuration of a time input field in Splunk, showing how a user-defined token is mapped to a specific search query.

**User defined token:** A yellow callout points to the `token="time_tok"` attribute in the input field's HTML code.

**Predefined modifiers to capture the time range:** A yellow callout points to the `$time_tok.earliest$` and `$time_tok.latest$` placeholders in the search string, which are used to capture the time range specified in the input field.

**Panel's Search Settings:** A yellow callout points to the "Time Range" dropdown in the "Edit Search" panel, which is set to "Shared Time Picker (time\_tok)".

**Input Settings:** The "Token" field is set to `time_tok`, and the "Default" field is set to "Last 7 days".

**Code Snippets:**

```


    <label></label>
    <default>
        <earliest>-7d@h</earliest>
        <latest>now</latest>
    </default>
<query>index=sales sourcetype=access_combined | timechart count
    <earliest>$time_tok.earliest$</earliest>
    <latest>$time_tok.latest$</latest>
</query>

```

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Time Input – Example 2

**Time Input - Example**

Global - No Token      Shared Time Picker - TimeTok1

Last 90 days      Last 30 days      Hide Filters

**1** Global - All Errors by Host

**2** Shared Time Picker - TimeTok1 - All Errors by Host

**3** Local - TimeTok2

TimeTok2

Last 7 days

All Errors by Host

**4** XML Time - <earliest>-3d@d</earliest>

All Errors by Host

**5** Query Time - earliest=-60m

All Errors by Host

...

```

<input type="time"
searchWhenChanged="true">
<label>Global - No Token</label>
<default>
<earliest>-90d@d</earliest>
<latest>now</latest>
</default>
</input>
...
<panel>
<title>Global</title>
<chart>
<title>All Errors by Host</title>
<search>
<query>sourcetype=access_combined
status>399 | timechart count(action)
by host
</query>
<sampleRatio>1</sampleRatio>
</search>
...

```

...

```

<input type="time" token="TimeTok1" searchWhenChanged="true">
<label>Shared Time Picker - TimeTok1</label>
<default>
<earliest>-30d@h</earliest>
<latest>now</latest>
</default>
</input>
...
<panel>
<title>Shared Time Picker - TimeTok1</title>
<chart>
<title>All Errors by Host</title>
<search>
<query>sourcetype=access_combined status>399
| timechart count(action) by host</query>
<earliest>$TimeTok1.earliest$</earliest>
<latest>$TimeTok1.latest$</latest>
<sampleRatio>1</sampleRatio>
</search>
...

```

...

```

<input type="time" token="TimeTok2" searchWhenChanged="true">
<label>TimeTok2</label>
<default>
<earliest>-7d@d</earliest>
<latest>now</latest>
</default>
</input>
...
<chart>
<title>All Errors by Host</title>
<search>
<query>sourcetype=access_combined status>399
| timechart count(action) by host</query>
<earliest>$TimeTok2.earliest$</earliest>
<latest>$TimeTok2.latest$</latest>
<sampleRatio>1</sampleRatio>
</search>
...

```

...

...

```

<panel>
<title>Query Time - earliest=-60m</title>
<chart>
<title>All Errors by Host</title>
<search>
<query>sourcetype=access_combined
status>399 earliest=-60m | timechart
count(action) by host
</query>
<earliest>-7d</earliest>
<latest>now</latest>
<sampleRatio>1</sampleRatio>
</search>
...

```

5

...

```

<panel>
<title>XML Time - <earliest>-3d@d</earliest></title>
<chart>
<title>All Errors by Host</title>
<search>
<query>sourcetype=access_combined
status>399 | timechart
count(action) by host
</query>
<earliest>-3d@d</earliest>
<latest>now</latest>
<sampleRatio>1</sampleRatio>
</search>
...

```

4

# TextInput Example

**Text Input - Example**

Enter product name:

All Vendor Sales

4,000

2,000

count

Tue Aug 7 2018 Sat Aug 11

```
...
<fieldset submitButton="false">
  <input type="text" token="p_name_tok" searchWhenChanged="true">
    <label>Enter product name:</label>
    <default>*</default>
    <prefix></prefix>
    <suffix></suffix>
  </input>
</fieldset>
<row>
  <panel>
    <chart>
      <title>All Vendor Sales</title>
      <search>
        <query>sourcetype="vendor_sales" product_name=$p_name_tok$</query>
        | timechart count</query>
      <earliest>-30d@d</earliest>
      <latest>now</latest>
    </search>
  ...

```

Use a name that identifies your token as a token

Use \$...\$ delimiters to access a token value

**Input Settings**

**T Text**

General

Label Enter product name:

Search on Change

Token Options

Token ? p\_name\_tok

Default ? \*

Initial Value ?

Token Prefix ? "

Token Suffix ? "

Cancel Apply

# Dropdown Menu Example

**Dropdown Menu - Example**

Select a product:

Benign Space Debris ▾ Last 30 days

**Benign Space Debris**

Date	Count
Tue Aug 7 2018	~800
Thu Aug 9	~800
Sat Aug 11	~800
Mon Aug 13	~700
We	~500

```
...
<fieldset submitButton="false" autoRun="false">
  <input type="dropdown" token="prod_name_tok" searchWhenChanged="true">
    <label>Select a product:</label>
    <choice value="*>All</choice>
    <search>
      <query>| inputlookup bcg_products</query>
      <earliest>-7d@h</earliest>
      <latest>now</latest>
    </search>
    <default*></default>
    <fieldForLabel>product_name</fieldForLabel>
    <fieldForValue>product_name</fieldForValue>
    <initialValue>*</initialValue>
  </input>
  <input type="time" token="time_tok">
    <label></label>
    <default>
      <earliest>-7d@h</earliest>
      <latest>now</latest>
    </default>
  </input>
</fieldset>
<row>
  <panel>
    <chart>
      <title>$prod_name_tok$</title>
      <search>
        <query>sourcetype=access_combined product_name="$prod_name_tok$"
          | timechart count</query>
        <earliest>$time_tok.earliest$</earliest>
        <latest>$time_tok.latest$</latest>
      </search>
    ...
  
```

**Input Settings**

User defined token

Query uses an input lookup

Define a default menu selection

Access the value using \$...\$ delimiters

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Multiselect Input Example

**Multiselect Input - Example**

Select a category

SIMULATION X SPORTS X STRATEGY X Last 7 days

All Vendor Sales

750  
500  
250

Thu Aug 30 2018 Fri Aug 31 Sat Sep 1 Sun

SIMU

```
...
<fieldset submitButton="false" autoRun="false">
<input type="multiselect" token="categoryId_tk" searchWhenChanged="true">
  <label>Select a category</label>
  <choice value="*>All</choice>
  <search>
    <query>| inputlookup bcg_products | stats count by categoryId</query>
    <earliest>-7d@h</earliest>
    <latest>now</latest>
  </search>
  <fieldForLabel>categoryId</fieldForLabel>
  <fieldForValue>categoryId</fieldForValue>
  <default>*</default>
  <prefix></prefix>
  <valuePrefix>categoryId=</valuePrefix>
  <valueSuffix>"</valueSuffix>
  <delimiter> OR </delimiter>
  <suffix></suffix >
</input>
</fieldset>
<row>
  <panel>
    <chart>
      <title>All Vendor Sales</title>
      <search>
        <query>sourcetype="access_combined" $categoryId_tk$ | timechart count by categoryId usenull=f</query>
        <earliest>$time_tk.earliest$</earliest>
        <latest>$time_tk.latest$</latest>
      </search>
    ...

```

User defined token

Query uses an input lookup

Token prefix, suffix, and delimiter

**Input Settings**

T Text  Radio  Dropdown

Search on Change

Label Select a category

Token Options

Token ? categoryId\_tk

Default ? All

Initial Value ? Select...

Token Prefix ? (

Token Suffix ? )

Token Value Prefix ? categoryId=\*

Token Value Suffix ? \*

Delimiter ? OR

Preview categoryId="value1" OR categoryId="value2" OR ...

Static Options

Name	Value
All	*

+ Add New

Dynamic Options

Content Type

Search String

Run Search

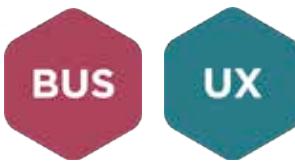
Last 7 days

Field For Label ? categoryId

Field For Value ? categoryId

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Cascading Inputs



## Cascading Inputs Example

Country      State/Province      City

All 1      All 2      All 3

Use the selection of one input to reduce or set the values of another

Note 

Use an event handler to reset a menu when another menu is changed. Event handlers are discussed in module 6.

```
...
<fieldset submitButton="false">
  <input type="dropdown" token="v_country_tok" searchWhenChanged="true">
    <label>Country</label>
    <choice value="*>All</choice>
    <default>*</default>
    <fieldForLabel>VendorCountry</fieldForLabel>
    <fieldForValue>VendorCountry</fieldForValue>
    <search>
      <query>| inputlookup bcg_vendors | search VendorStateProvince=$v_state_tok|$ VendorCity=$v_city_tok|$</query>
      | dedup VendorCountry
      | fields VendorCountry
      | sort VendorCountry</query>
    <earliest>-24h@h</earliest>
    <latest>now</latest>
  </search>
</input>
<input type="dropdown" token="v_state_tok" searchWhenChanged="true">
  <label>State/Province</label>
  <choice value="*>All</choice>
  <default>*</default>
  <fieldForLabel>VendorStateProvince</fieldForLabel>
  <fieldForValue>VendorStateProvince</fieldForValue>
  <search>
    <query>| inputlookup bcg_vendors | search VendorCountry=$v_country_tok|$ VendorCity=$v_city_tok|$</query>
    | dedup VendorStateProvince
    | fields VendorStateProvince
    | sort VendorStateProvince</query>
  <earliest>-24h@h</earliest>
  <latest>now</latest>
  </search>
</input>
<input type="dropdown" token="v_city_tok" searchWhenChanged="true">
  <label>City</label>
  <choice value="*>All</choice>
  <default>*</default>
  <fieldForLabel>VendorCity</fieldForLabel>
  <fieldForValue>VendorCity</fieldForValue>
  <search>
    <query>| inputlookup bcg_vendors | search VendorCountry=$v_country_tok|$ VendorStateProvince=$v_state_tok|$</query>
    | dedup VendorCity
    | fields VendorCity
    | sort VendorCity</query>
  <earliest>-24h@h</earliest>
  <latest>now</latest>
  </search>
  <allowCustomValues>true</allowCustomValues>
</input>
</fieldset>
```

# Token Filters



Token filters ensure that you correctly capture a token's value

Built-in	
\$token_name s\$	Wrap value in quotes
\$token_name h\$	Escape any HTML in value
\$token_name u\$	Encode URL values
\$token_name n\$	No encode
\$\$token_name\$\$	Escape the \$ token delimiter character
Custom	
\$token_name myFilter\$	Build your own token filters in JavaScript



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Token Filters – Example 1

Use the `|s` filter to add quotation marks around the returned value

```
...
<search>
<query>index=bcg_index sourcetype=$srctyp Tok|s$ | timechart count by sourcetype</query>
<earliest>-30d@d</earliest>
<latest>now</latest>
<sampleRatio>1</sampleRatio>
</search>
...
```



```
index=bcg_index sourcetype="access_combined" | timechart count by sourcetype
```

# Token Filters – Example 2

Use the `|n` filter to not encode

```
...
<search>
  <query>index=news sourcetype=$media_tok$ | table sourcetype title link
  </query>
  <earliest>$time_tok.earliest$</earliest>
  <latest>$time_tok.latest$</latest>
  <sampleRatio>1</sampleRatio>
</search>
<option name="count">20</option>
<option name="wrap">true</option>
<drilldown>
  <link target="_blank"> $row.link|n$ </link>
</drilldown>
...

```

<https://www.nytimes.com/2017/10/16/technology/personaltech/macos-high-sierra-upgrade.html?partner=rss&emc=rss>

```
...
<search>
  <query>index=news sourcetype=$media_tok$ | table sourcetype title link
  </query>
  <earliest>$time_tok.earliest$</earliest>
  <latest>$time_tok.latest$</latest>
  <sampleRatio>1</sampleRatio>
</search>
<option name="count">20</option>
<option name="wrap">true</option>
<drilldown>
  <link target="_blank"> $row.link$ </link>
</drilldown>
...

```

<http://52.12.61.149/en-US/app/search/https%3A%2F%2Fwww.nytimes.com%2F2017%2F10%2F16%2Ftechnology%2Fpersonaltech%2Fmacos-high-sierra-upgrade.html%3Fpartner%3Drss%26emc%3Drss>

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Global Environment Tokens



\$env:user\$

\$env:user\_realname\$

\$env:user\_email\$

\$env:app\$

\$env:locale\$

\$env:page\$

\$env:product\$

\$env:version\$

\$env:view\_label\$

\$env:is\_enterprise\$

## Global Tokens

### Default Environmental Tokens

Currently logged in user = admin

Full name of logged in user = Administrator

Email address of logged in user = changeme@example.com

Splunk app name = advdash\_slides

Current locale UI internationalization = \$env:locale\$

Current page name = global\_tokens\_xml

Current view label = Global Tokens

Splunk Core products = enterprise

Splunk version number = 7.3.0

Is this Splunk Enterprise = true

```
...
<panel>
<title>Default Environmental Tokens</title>
<html>
<p>Currently logged in user = $env:user$</p>
<p>Full name of logged in user = $env:user_realname$</p>
<p>Email address of logged in user = $env:user_email$</p>
<p>Splunk app name = $env:app$</p>
<p>Current locale UI internationalization = $env:locale$</p>
<p>Current page name = $env:page$</p>
<p>Current view label = $env:view_label$</p>
<p>Splunk Core products = $env:product$</p>
<p>Splunk version number = $env:version$</p>
<p>Is this Splunk Enterprise = $env:is_enterprise$</p>
</html>
</panel>
...

```

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Useful References

- Token Usage in dashboards

[docs.splunk.com/Documentation/Splunk/latest/Viz/tokens](https://docs.splunk.com/Documentation/Splunk/latest/Viz/tokens)

- Token Filters

[docs.splunk.com/Documentation/Splunk/latest/Viz/tokens#Token\\_filters](https://docs.splunk.com/Documentation/Splunk/latest/Viz/tokens#Token_filters)

- Create and Edit Forms

[docs.splunk.com/Documentation/Splunk/latest/Viz/FormEditor](https://docs.splunk.com/Documentation/Splunk/latest/Viz/FormEditor)

The screenshot shows the Splunk Enterprise Documentation website. At the top right, there is a "Version" dropdown set to "Latest release". The main title is "Splunk® Enterprise" with "Manuals" above it. Below the title, it says "Splunk Enterprise is the data collection, indexing, and visualization engine for operational intelligence." A navigation bar at the bottom includes "Get started", "Search and report" (which is highlighted in dark grey), "Administer", "Deploy", and "Develop". To the right of the navigation bar, there are several links: "Alerting Manual", "Reporting Manual", "Metrics", "Dashboards and Visualizations", "Search Manual", "Knowledge Manager Manual", "Search Reference", and "Pivot Manual". Each link has a brief description below it.

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Lab 2 – Add Interactivity

Time: 40 minutes

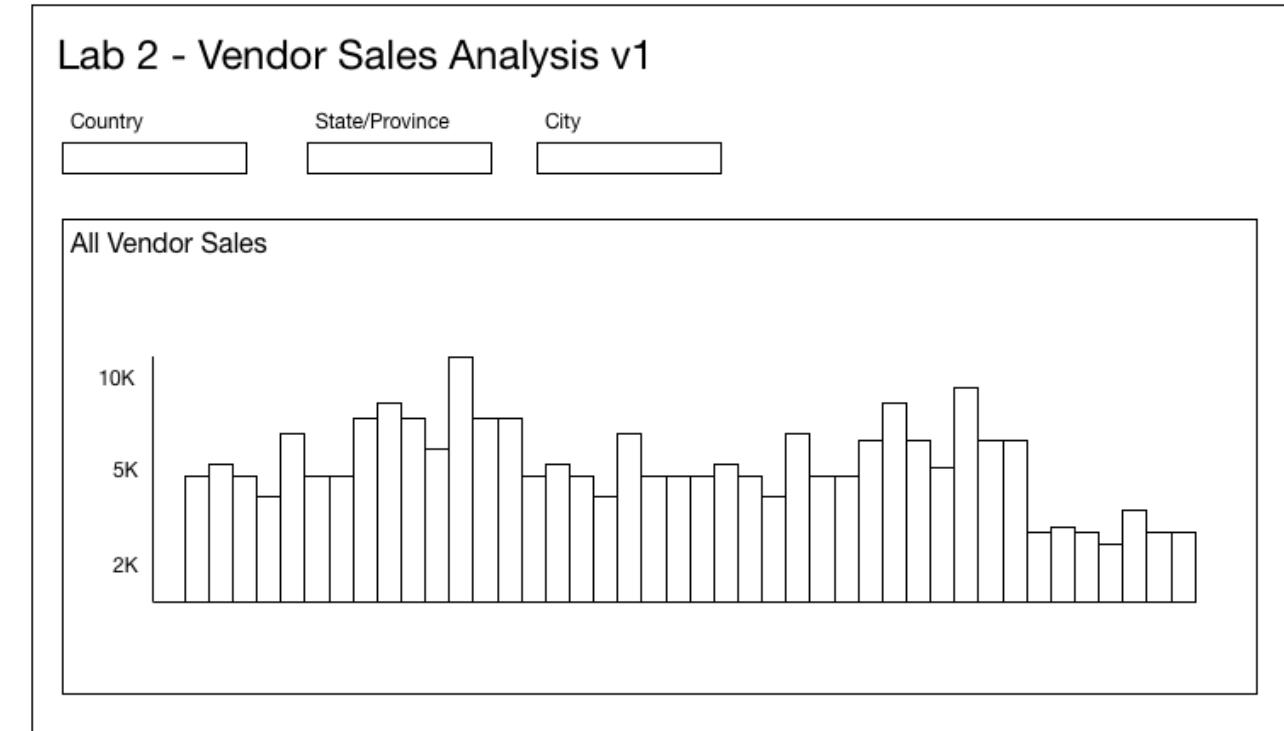
**Scenario:** The sales team is impressed with the new server errors dashboard. They would like to add a form to their app. The form should display a column chart of vendor data based on user input for country, state or province, and city.

**Tasks:**

- Create a form
- Add a token filter
- Add cascading inputs

**Challenge Task (optional):**

- Add an event handler to reset menus



# Module 3: Improving Performance

Generated for Matt Brown ([mbrown@idbny.com](mailto:mbrown@idbny.com)) (C) Splunk Inc, not for distribution

# Module Objectives

---

- Identify ways to improve dashboard performance
- Describe techniques to improve search efficiency
- Name two ways to accelerate a search
- Use the tstats command with a global search
- Use a post-process search

# Improving Performance



- Refine searches
- Use scheduled reports
- Accelerate reports
- Accelerate data models
- Use the tstats command
- Use a global search
- Use tokens



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Refining Searches



- Limit your search to a specific time window and quantity of data retrieved
- Use the most efficient command for the use case
  - transaction vs. stats
  - tstats
- Make the base search part of a global search, as specific as possible
- Avoid using NOT expressions

```
... | transaction trade_id | chart count by duration
```

```
... | stats range(_time) as duration by trade_id  
| chart count by duration
```

```
...  
<search>  
  <query>index=_internal $user$ | timechart $metric $($what$) by $group$</query>  
  <earliest>-30d@d</earliest>  
  <latest>now</latest>  
...  
<search>
```

```
  <query>| tstats $metric $($what$) from datamodel=foo where $user$ by all.$group$  
  | prestats=t summariesonly=t | timechart $metric $($what$) by $group$</query>  
  <earliest>-30d@d</earliest>  
  <latest>now</latest>  
...
```

# Using Scheduled Reports

- Avoid inline searches
- Schedule to run every 5 or 10 minutes or less frequently
- Prevent a flood of search jobs when dashboards are loaded

The image shows two side-by-side 'Edit Schedule' dialog boxes from the Splunk interface. Both dialogs have a 'Report' field set to 'bcg\_ws\_errors\_by\_host' and a 'Schedule Report' checkbox checked.

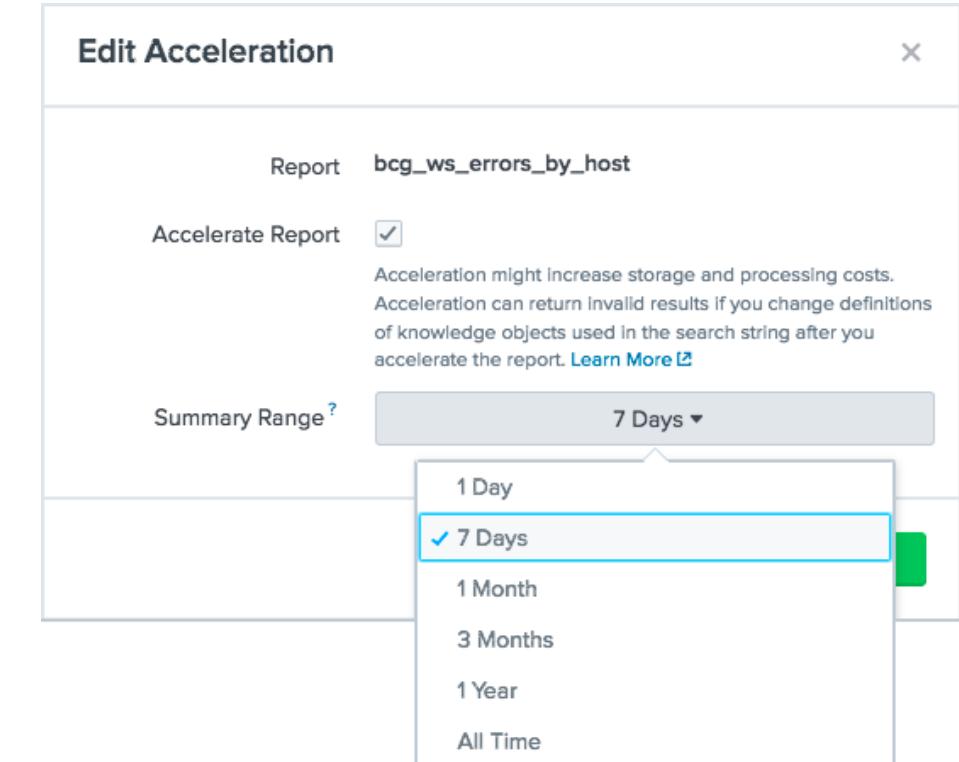
- Left Dialog:**
  - Schedule: 'Run on Cron Schedule'
  - Cron Expression: `*/30 * * * *`
  - Time Range: 'Last 30 days'
  - Schedule Priority: 'Default'
  - Schedule Window: '15 minutes'
  - Trigger Actions: '+ Add Actions'
- Right Dialog:**
  - Schedule: 'Run every week'
  - On: 'Monday' at '6:00'
  - Time Range: 'Last 30 days'
  - Schedule Priority: 'Default'
  - Schedule Window: '15 minutes'
  - Trigger Actions: '+ Add Actions'

Cron Parameter	Schedule
<code>*/5 * * * *</code>	Every 5 minutes
<code>*/30 * * * *</code>	Every 30 minutes
<code>0 */12 * * *</code>	Every 12 hours, on the hour
<code>*/20 * * * 1-5</code>	Every 20 minutes, Monday through Friday
<code>0 9 1-7 * 1</code>	First Monday of each month, at 9am.

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Accelerating Reports

- Automatically creates summaries to speed completion times
- Periodically ages out data
- Data is stored on the indexers
- Search must meet three criteria:
  - Uses a transforming command
  - Commands before the first transforming command, must be streamable
  - Cannot use event sampling



## Note

Report acceleration only works for reports that have Search Mode set to Smart or Fast.

# Accelerating Data Models

- Accelerates all fields defined in the data model
- Creates time-series index (TSIDX) files
- Updates every five minutes
- Only administrators can enable acceleration
- Anyone can search using an accelerated data model
- Most efficient when root event dataset includes the index in the initial constraint search

The screenshot shows the Splunk Data Models interface. In the top navigation bar, it says "25 Data Models" and "App: Search & Reporting (search)". On the right, there are filters for "Created in the App". Below the header, a table lists data models with columns for Title, Type, and Actions. One row for "Buttercup Games Online Sales" is selected. A context menu is open over this row, with "Edit Datasets" highlighted in blue and "Edit Acceleration" highlighted in green. A modal window titled "Edit Acceleration" is open, showing the following details:

- Data Model: Buttercup Games Online Sales
- Accelerate:  (with a note: "Acceleration may increase storage and processing costs.")
- Summary Range: 3 Months

At the bottom of the modal are "Cancel" and "Save" buttons.

# tstats Command

- Generating command
- Use to search data models or data model objects
- Perform statistical queries on indexed fields in tsidx files
  - Also against indexed fields like source, host, sourcetype, and index
- Wildcard characters are not supported in field values in aggregate functions or BY clauses

```
| tstats [prestats=boolean] [summariesonly=boolean] <stats-function> [FROM datamodel=<datamodel-name>] [BY field-list]
```

↑  
Use to pipe results  
to chart, stats or  
timechart

↑  
Use to generate  
results from  
TSIDX data

↑  
Perform a basic count  
of a field or a function  
on a field

↑  
Specify the filename  
(object ID) of an  
accelerated data model

↑  
Specify one or  
more fields to  
group results

# tstats Command – Arguments

- **prestats=<boolean>**
  - true allows you to pipe the data to **chart**, **stats**, or **timechart**
    - ▶ Prevents renaming the result using the AS keyword
  - false is the default
  - Enables **append=t** where the results append to existing results instead of generating them

```
| tstats [prestats=boolean] [summariesonly=boolean] <stats-function> [FROM datamodel=<datamodel-name>] [BY field-list]
```

# tstats Command – Arguments (cont.)

- **summariesonly=boolean**

- Applies only to an accelerated data model
- **true** generates results from the accelerated data model's TSIDX data
- **false** (default) generates results from both summarized (accelerated data model TSIDX data) and non-summarized data
  - May cause a larger result count if: some of the data has not yet been added to the summary OR has been aged out of it

```
| tstats [prestats=boolean] [summariesonly=boolean] <stats-function> [FROM datamodel=<datamodel-name>] [BY field-list]
```

# tstats Command – Functions

- **stats-function**

- Perform a basic count or a function on a field
- Perform any number of aggregates
- Can rename the result using AS

Type	Supported functions and syntax				
<b>Aggregate functions</b>	avg() count() distinct_count() estdc()	exactperc<int>() max() median() min() mode()	perc<int>() range() stdev() stdevp()	sum() sumsq() upperperc<int>() var() varp()	
<b>Event order functions</b>	earliest()	first()	last()		latest()
<b>Multivalue stats and chart functions</b>	values(x)				

```
| tstats [prestats=bool] [summariesonly=bool] <stats-function> [FROM datamodel=<datamodel-name>] [BY field-list]
```

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# tstats Command – Clause Arguments

- **FROM datamodel=<datamodel-name>**
  - Accesses an accelerated data model's summaries
- **WHERE <search-query>**
  - Specify a search
  - Can specify a set of values with the IN operator
- **BY <field-list>**
  - You must specify a field-list
  - If you used to group by \_time, use span to group the time buckets
  - Cannot use wildcards

```
| tstats [prestats=boolean] [summariesonly=boolean] <stats-function> [FROM datamodel=<datamodel-name>] [BY field-list]
```

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# tstats Command – Example



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Use a Global Search

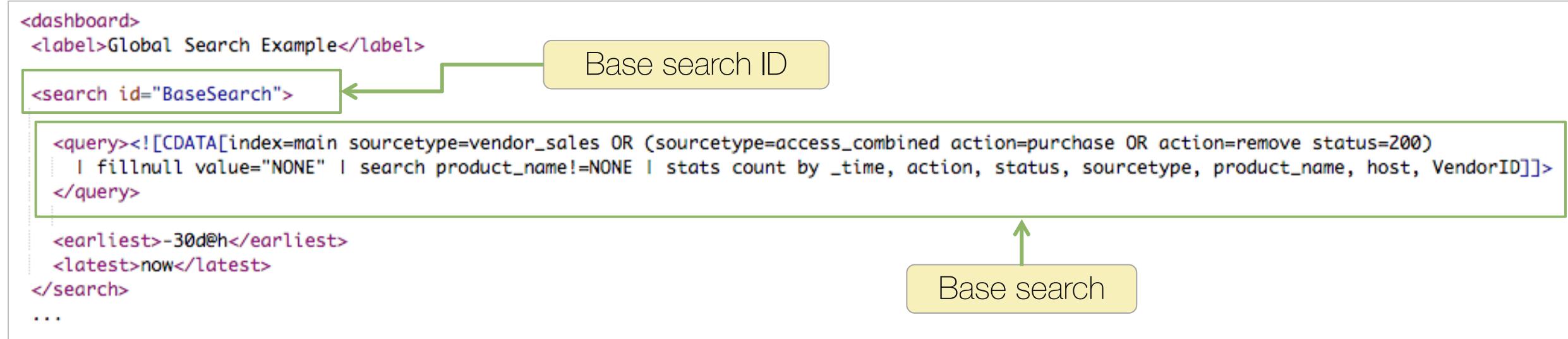


- Global search: a **single** base search with post-process searches that populate all panels on a dashboard or form
- Base search: `<search id="myBaseSearch">`
  - Provides the input for post-process searches
  - Typically a dedicated search not in a panel
  - Can be any inline search or report on a dashboard
  - `<search id=myBaseSearch ref=myReport>`
  - Use a transforming command to avoid the 10,000 results limit that can be passed to a post-process search
- Post-process search: `<search base="myBaseSearch">`
  - Perform additional processing on base search results
  - Can populate form inputs

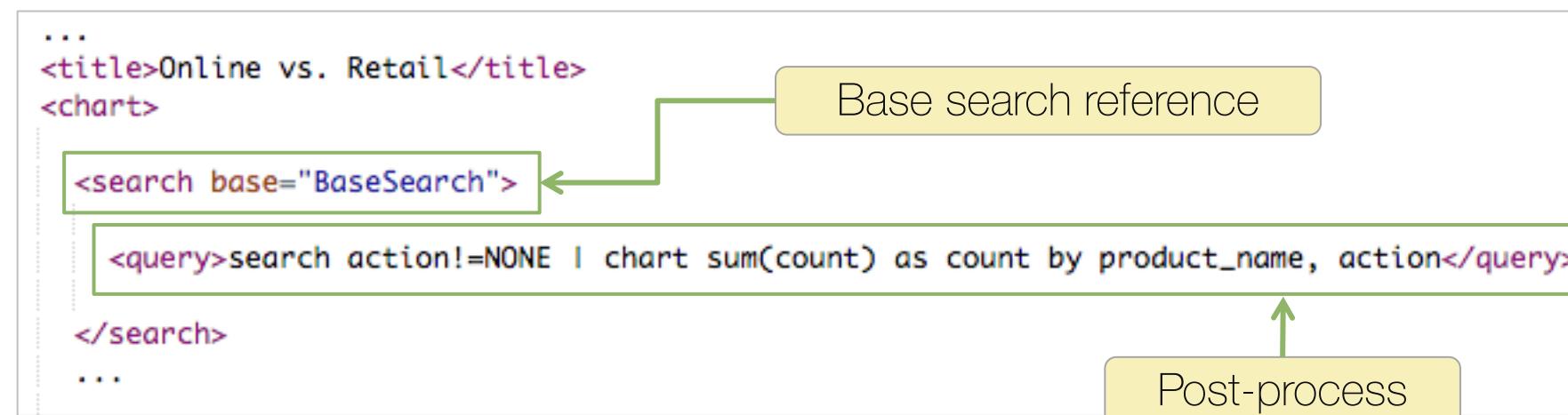
**Warning**   
Passing a large number of search results from a base search can cause a server time out.

# Use a Global Search (cont.)

- The base search gathers statistics for the downline processing



- The post process performs further processing of results



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Global Search – Null Values

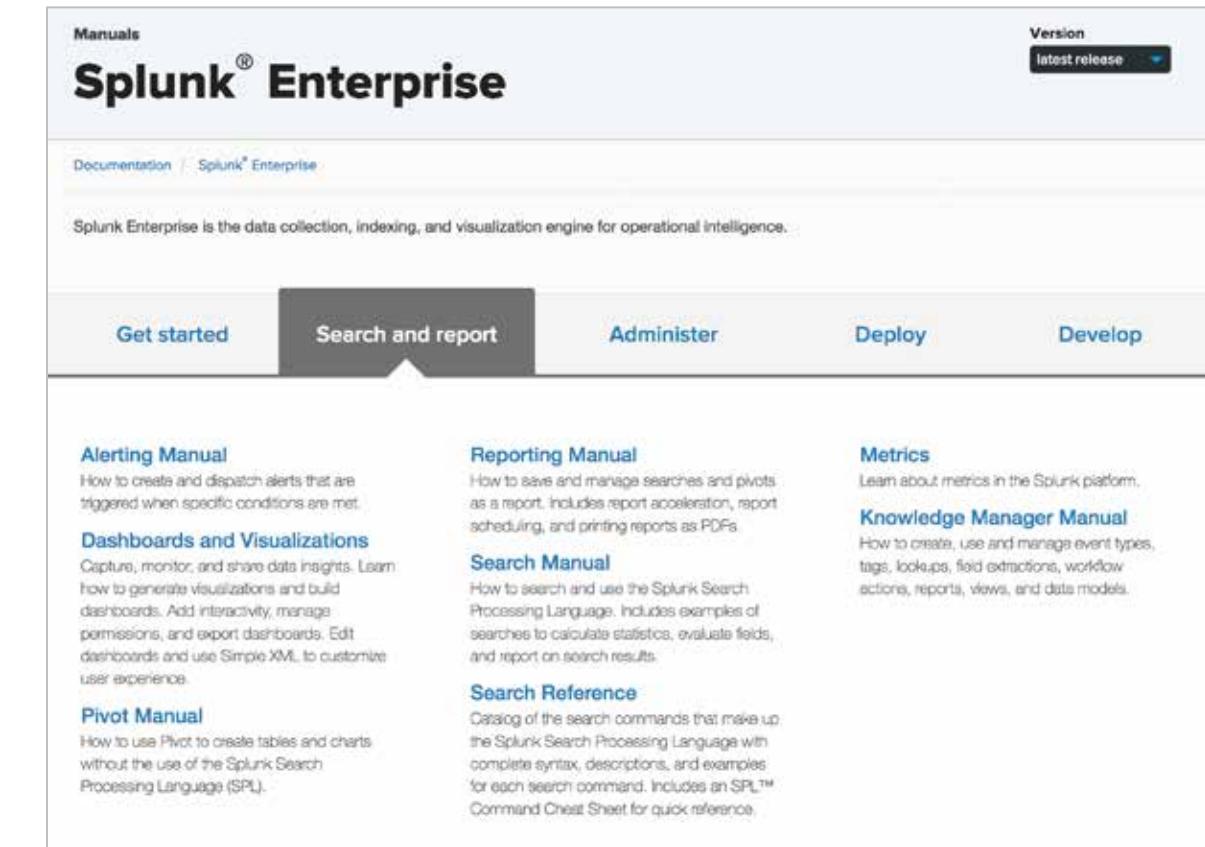
- Make sure all fields identified in a base search have a value
- Remove or include null values as required in the post-process

```
...
<search id="baseSearch">
    <query>index=bcg_index sourcetype=access_combined | fillnull value="NONE"
        | stats count by _time, sourcetype, action, status, product_name, host</query>
    <earliest>-30d@d</earliest>
    <latest>now</latest>
</search>
<row>
    <panel>
        <chart>
            <title>Purchases & Lost Sales</title>
            <search base="baseSearch">
                <query>search product_name!=NONE action!=NONE AND (action=purchase OR action=remove)
                    | chart sum(count) as count by product_name, action
                    | rename product_name as "Product Name", remove as "Lost Sales", purchase as Purchases</query>
            </search>
        ...
    ...
</row>
```

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Useful References

- Search Reference – tstats  
[docs.splunk.com/Documentation/Splunk/latest/SearchReference/Tstats](https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Tstats)
- Searches Power Dashboards and Forms  
[docs.splunk.com/Documentation/Splunk/latest/Viz/Savedsearches](https://docs.splunk.com/Documentation/Splunk/latest/Viz/Savedsearches)
- Dashboards & Visualizations Manual  
[docs.splunk.com/Documentation/Splunk/latest/Viz/Aboutthismanual](https://docs.splunk.com/Documentation/Splunk/latest/Viz/Aboutthismanual)



The screenshot shows the Splunk Enterprise Documentation homepage. At the top right, there is a "Version" dropdown set to "Latest release". The main title is "Splunk® Enterprise" with "Manuals" above it. Below the title, it says "Splunk Enterprise is the data collection, indexing, and visualization engine for operational intelligence." A navigation bar below the title includes "Get started", "Search and report" (which is highlighted in dark grey), "Administer", "Deploy", and "Develop". To the right of the navigation bar, there are two columns of documentation links:

- Alerting Manual**: How to create and dispatch alerts that are triggered when specific conditions are met.
- Reporting Manual**: How to save and manage searches and pivots as a report. Includes report acceleration, report scheduling, and printing reports as PDFs.
- Dashboards and Visualizations**: Capture, monitor, and share data insights. Learn how to generate visualizations and build dashboards. Add interactivity, manage permissions, and export dashboards. Edit dashboards and use Simple XML to customize user experience.
- Search Manual**: How to search and use the Splunk Search Processing Language. Includes examples of searches to calculate statistics, evaluate fields, and report on search results.
- Pivot Manual**: How to use Pivot to create tables and charts without the use of the Splunk Search Processing Language (SPL).
- Search Reference**: Catalog of the search commands that make up the Splunk Search Processing Language with complete syntax, descriptions, and examples for each search command. Includes an SPL™ Command Cheat Sheet for quick reference.

Below these sections, there are two more links: "Metrics" (Learn about metrics in the Splunk platform) and "Knowledge Manager Manual" (How to create, use and manage event types, tags, lookups, field extractions, workflow actions, reports, views, and data models).

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Lab 3 – Improve Performance

Time: 40 minutes

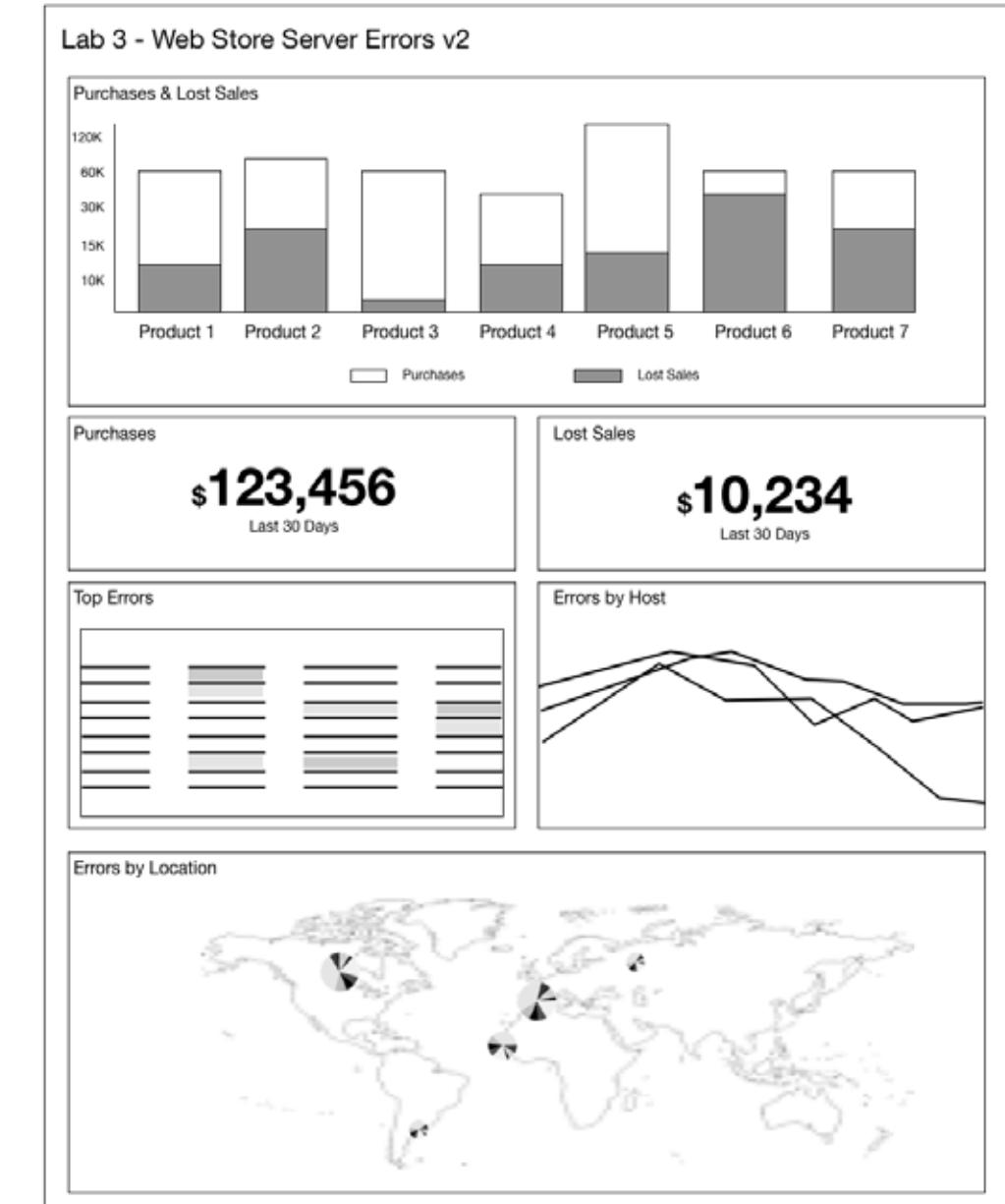
Scenario: Stakeholders have approved the prototype dashboard with some changes. They want it to load faster, have lower search overhead, and include two new panels that show the dollar amount of purchases and lost sales.

Tasks:

- Accelerate and schedule reports
- Create a dashboard
- Add a base search
- Add panels driven by post-process searches
- Add prebuilt panels and convert them to inline
- Accelerate the global search

Challenge Task (optional):

- Accelerate your data model
- Revise the base search to reference your data model



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Module 4: Customizing Dashboards

Generated for Matt Brown ([mbrown@idbny.com](mailto:mbrown@idbny.com)) (C) Splunk Inc, not for distribution

# Module Objectives

---

- Modify chart and panel colors
- Disable search access features
- Define Simple XML attributes
- Set panel refresh and delay times

# Customizing Views



- Dashboard Editor
  - Create and update dashboards and panels
- Customizing Simple XML
  - Chart and panel colors
  - Panel links
  - Panel refresh
  - Grouping panels

The screenshot illustrates the integration of the Splunk XML Editor and the Dashboard Editor. The top part shows the 'Edit Dashboard' interface with tabs for 'UI' and 'Source'. The 'Source' tab is selected, displaying XML code for a dashboard panel. A green arrow points from the XML code to the corresponding configuration in the 'Dashboard Editor' below. The 'Dashboard Editor' shows a bar chart titled 'All Sales by Product' with the Y-axis labeled 'totalSales' and the X-axis labeled 'product\_name'. The chart displays sales for various products, with 'Dread...usher' having the highest sales at approximately 160,000.

product_name	totalSales
Benig...ebrls	~40,000
Curling 2014	~45,000
Dread...usher	~160,000
Final Sequel	~65,000
Fire R...alone	~10,000
Holy ...ouda	~15,000
Mang... Bros.	~120,000
Mang...s Tee	~35,000
Medi...doms	~60,000
Orvilt...erine	~85,000
Puppl...mblies	~15,000
SIM Cubicle	~90,000
World...e Tee	~110,000
World...e Tee	~30,000

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Element Attributes



- Configure appearance and behavior of dashboards and forms
- Available for most Simple XML elements
  - <dashboard>, <form>, <fieldset>, <row>, <panel>, etc.
  - For example: <dashboard script="myScript">

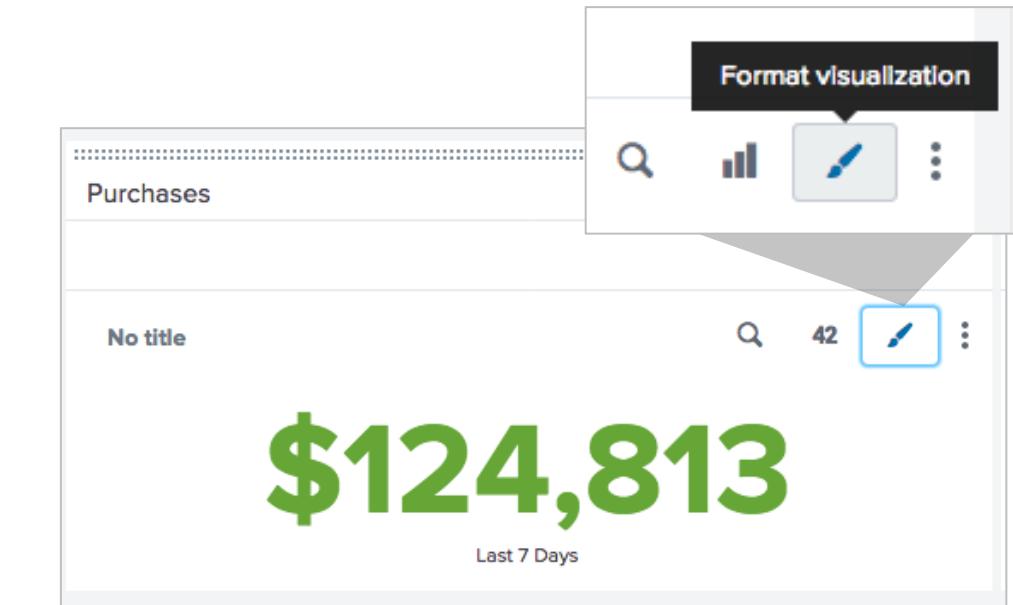
Attribute	Type	Description	Example
onunloadCancelJobs	boolean	Cancels search jobs when a user navigates away from the dashboard.	<dashboard onunloadCancelJobs="true">
script	string	Comma-separated list of custom .js files to load. The files must be in a folder or subfolder of the appserver/static directory.	<form script="myScript.js">
rejects	Comma-separated list	Prevent an element from rendering if one or more tokens in this list are defined.	<panel id="panel1" rejects="\$panel2\$">
depends	Comma-separated list	All tokens in the list must be defined for the element to render.	<chart id="column" depends="\$showCol\$">
id	text	Element identifier. Only alpha-numeric and underscore characters are valid.	<row id="row1">

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Chart Customization – Dashboard Editor



- Visualization Formatter
  - Change chart axis labels
  - Define color ranges
  - Options for each visualization



Single Value Visualization Options

General

Caption Last 7 Days

Color

Number Format

General

Use Colors Yes No

Color by Value Trend

Ranges from min to 1000 (red)

from 1000 to 2000 (orange)

from 2000 to max (green)

+ Add Range

Color Mode 42 42

General

Precision 0

Color

Use Thousand Separators Yes No

Number Format

Unit \$

Unit Position Before After

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Chart Customization – XML Editor

- Edit the panel XML directly to customize the appearance and behavior of your charts
  - Axis label text styles
  - Chart colors
  - Chart background and foreground colors
  - Chart height
  - Spacing between bars, columns, or clustered series

```
<option name="option name">value</option>
```

```
...
<option name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsisNone</option>
<option name="charting.axisLabelsX.majorLabelStyle.rotation">0</option>

<option name="charting.axisTitleX.visibility">visible</option>
<option name="charting.axisTitleY.visibility">visible</option>
<option name="charting.axisTitleY2.visibility">visible</option>

<option name="charting.axisX.abbreviation">none</option>
<option name="charting.axisX.scale">linear</option>
<option name="charting.axisY.abbreviation">none</option>
<option name="charting.axisY.scale">linear</option>
<option name="charting.axisY2.abbreviation">none</option>
<option name="charting.axisY2.enabled">0</option>
<option name="charting.axisY2.scale">inherit</option>

<option name="charting.chart">column</option>
<option name="charting.chart.bubbleMaximumSize">50</option>
<option name="charting.chart.bubbleMinimumSize">10</option>
<option name="charting.chart.bubbleSizeBy">area</option>

<option name="charting.chart.nullValueMode">gaps</option>
<option name="charting.chart.showDataLabels">none</option>
<option name="charting.chart.sliceCollapsingThreshold">0.01</option>
<option name="charting.chart.stackMode">stacked</option>
<option name="charting.chart.style">shiny</option>
<option name="charting.drilldown">none</option>

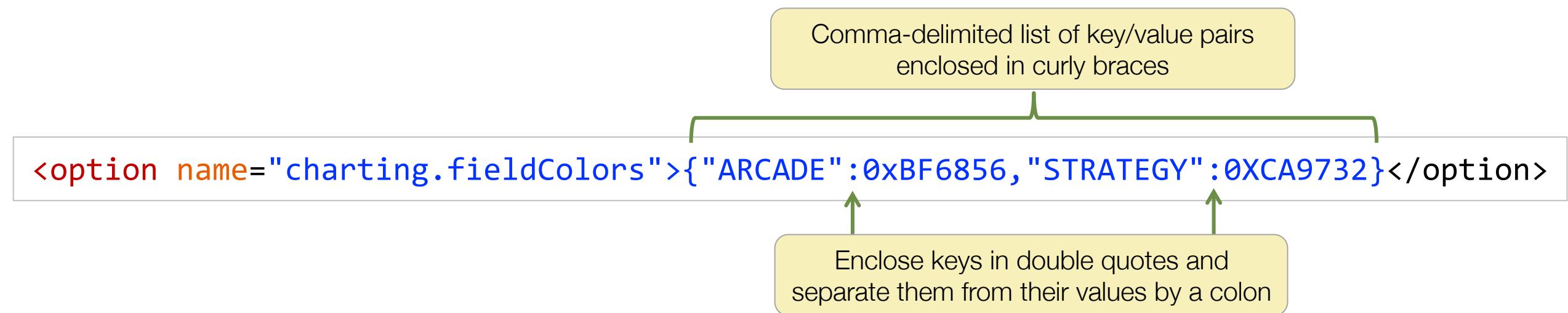
<option name="charting.layout.splitSeries">0</option>
<option name="charting.layout.splitSeries.allowIndependentYRanges">0</option>
<option name="charting.legend.labelStyle.overflowMode">ellipsisMiddle</option>
<option name="charting.legend.mode">standard</option>
<option name="charting.legend.placement">bottom</option>
<option name="charting.lineWidth">2</option>
</chart>
...
```

Chart Options Examples

# Chart Customization – XML Editor Example

- **charting.fieldColors**

- The map of hexadecimal color values to use for each field

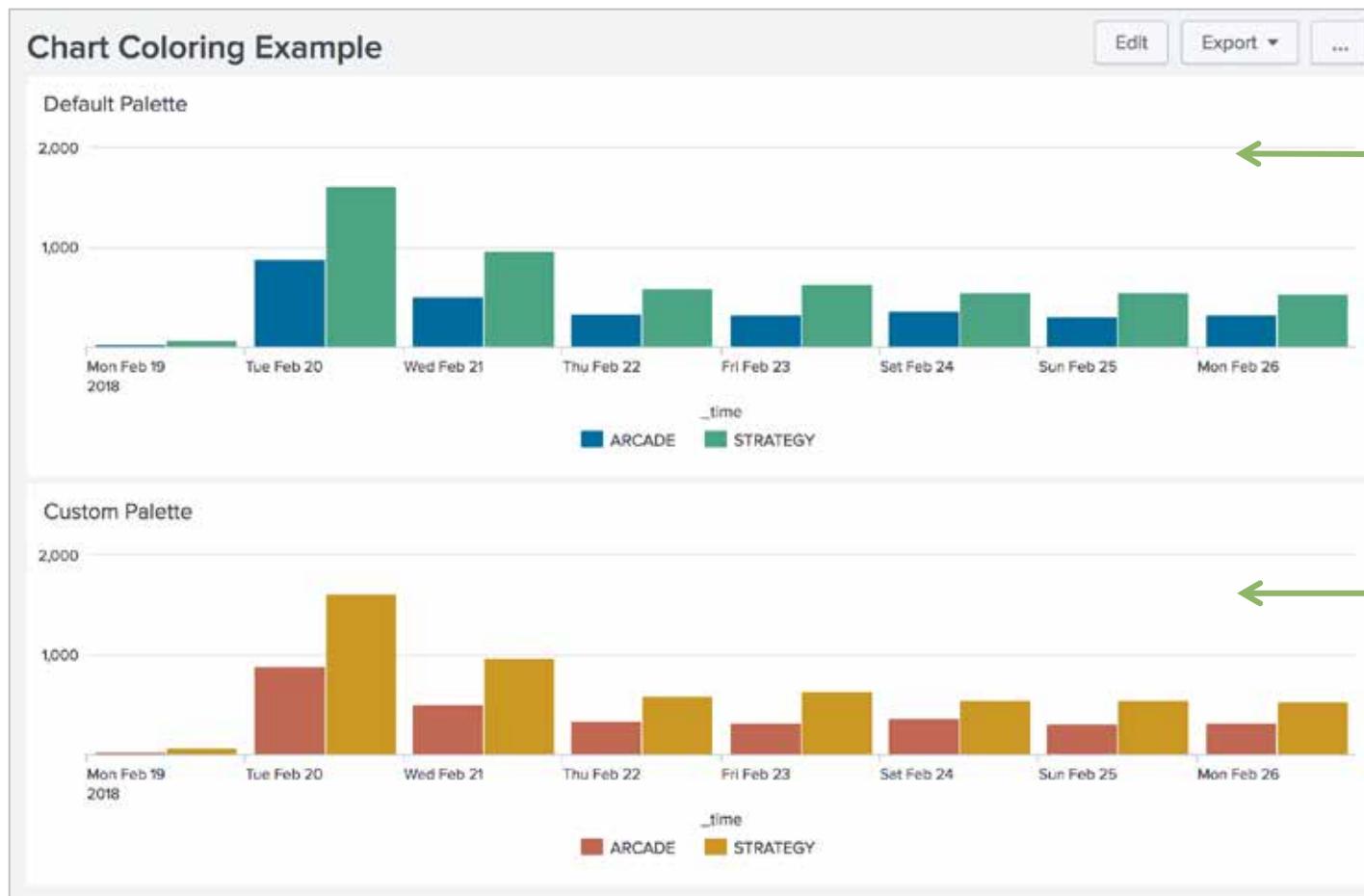


- Escape existing double quotes or backslashes or colons with a preceding backslash
- Escape special characters `\{\}(),:"` in a key or string value with double quotes

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Chart Customization – XML Editor Example (Cont.)

- 1 Add `charting.fieldColors` option
- 2 Add hexadecimal for each data series



```
<option name="charting.fieldColors">  
{"fieldname": hexcolor, "fieldname": hexcolor, ...}  
</option>
```

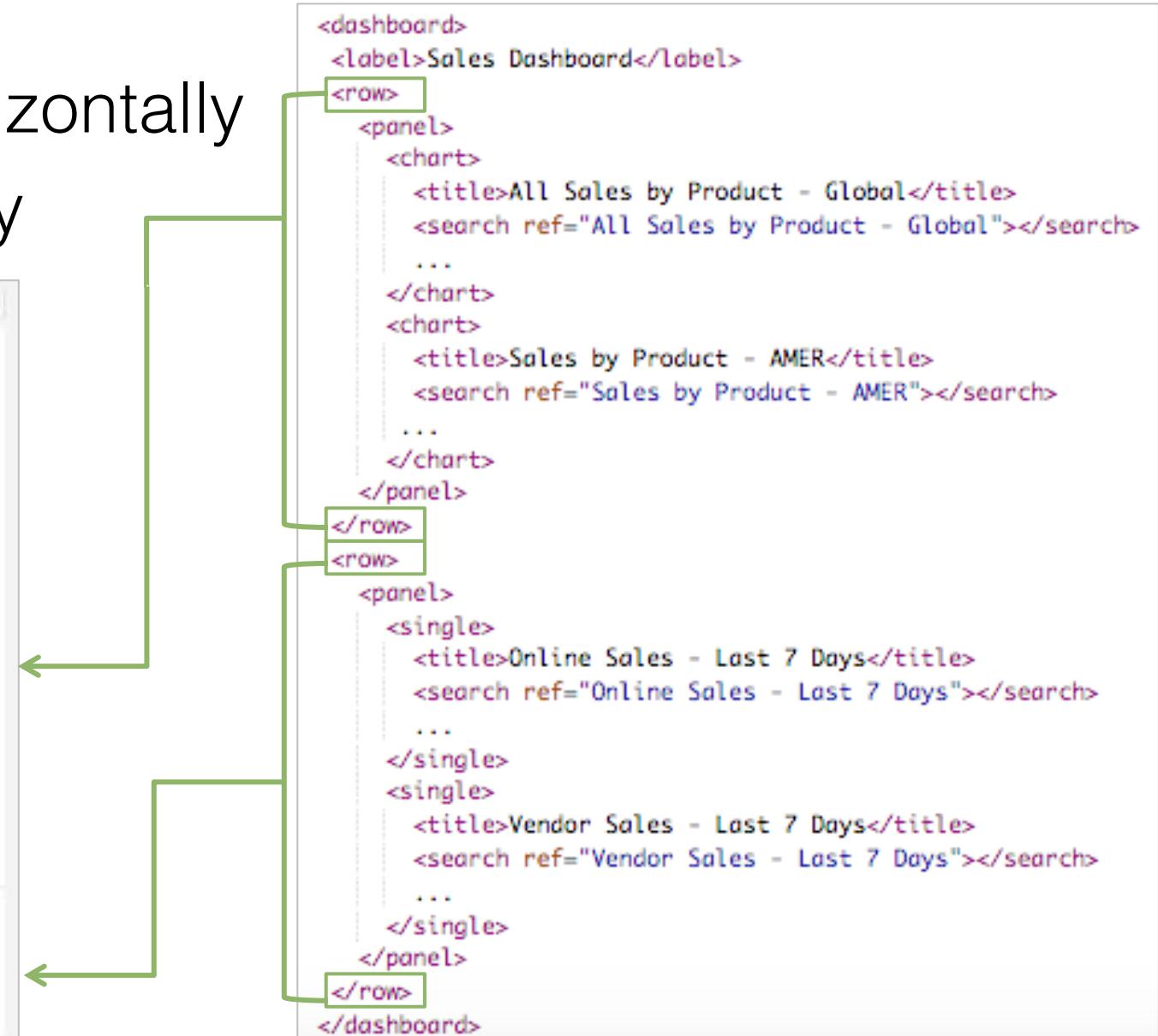
```
<dashboard>  
  <label>Chart Coloring Example</label>  
  <row>  
    <panel>  
      <title>Default Palette</title>  
      <chart>  
        <search ref="bcg_arcade_vs_strategy"></search>  
        ...  
        <option name="charting.legend.placement">bottom</option>  
      </chart>  
    </panel>  
  </row>  
  <row>  
    <panel>  
      <title>Custom Palette</title>  
      <chart>  
        <search ref="bcg_arcade_vs_strategy"></search>  
        ...  
        <option name="charting.legend.placement">bottom</option>  
        <option name="charting.fieldColors">  
          {"ARCADE":0xBF6856, "STRATEGY":0xCA9732}  
        </option>  
      </chart>  
    </panel>  
  </row>  
</dashboard>
```

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Grouping Visualizations



- <row>
  - Single value visualizations group horizontally
  - Default: visualizations group vertically

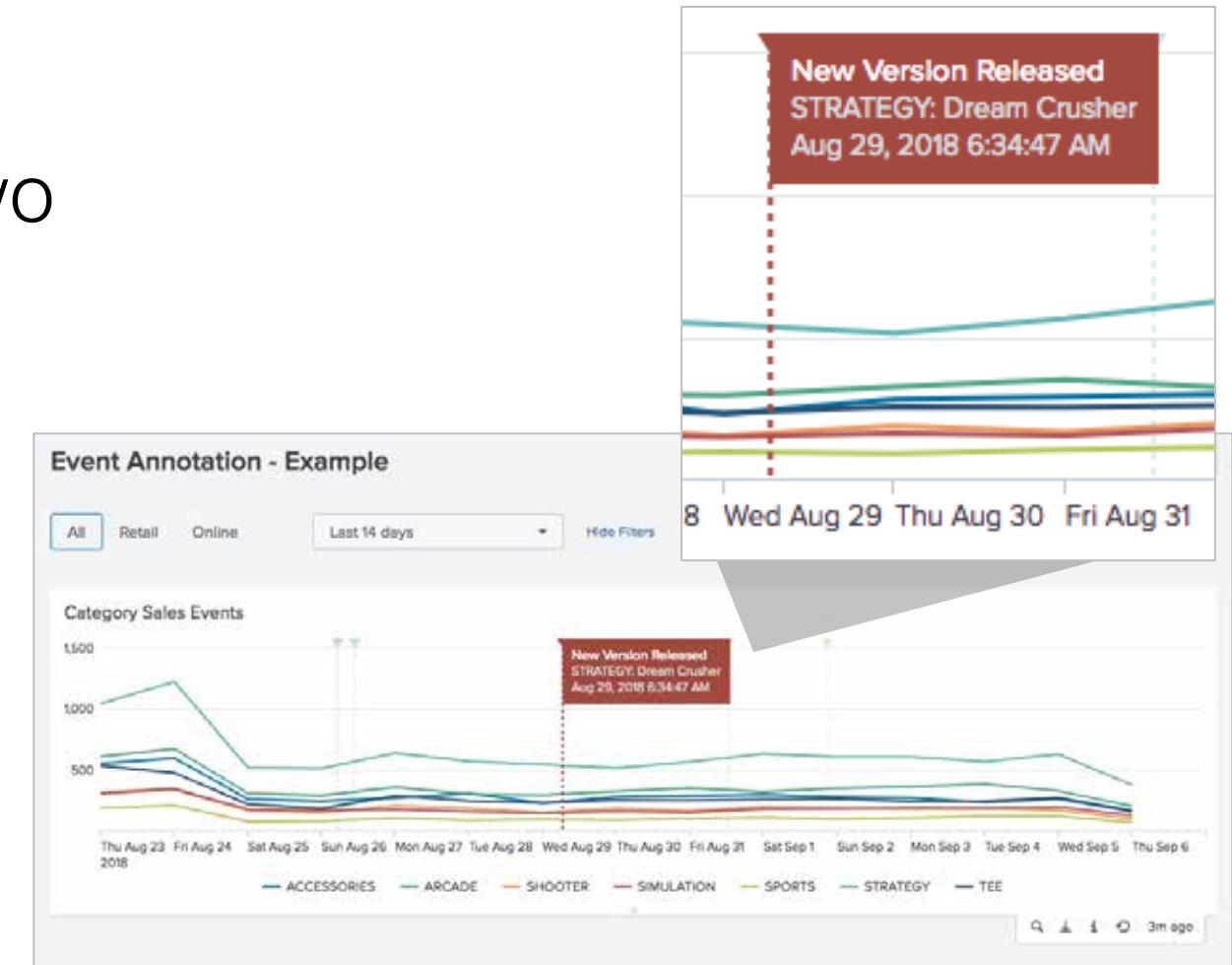


Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Event Annotation



- <search type="annotation">
- Annotate a time series visualization with two field values from another search or lookup
  - One value as a “label”
  - Second value as a “category”
- Displays as a callout
  - Annotation search \_time value matches a \_time value in the timeseries visualization
- Automatically filters for events matching the chart's time range



Note i  
PDF export is not available for event annotations.

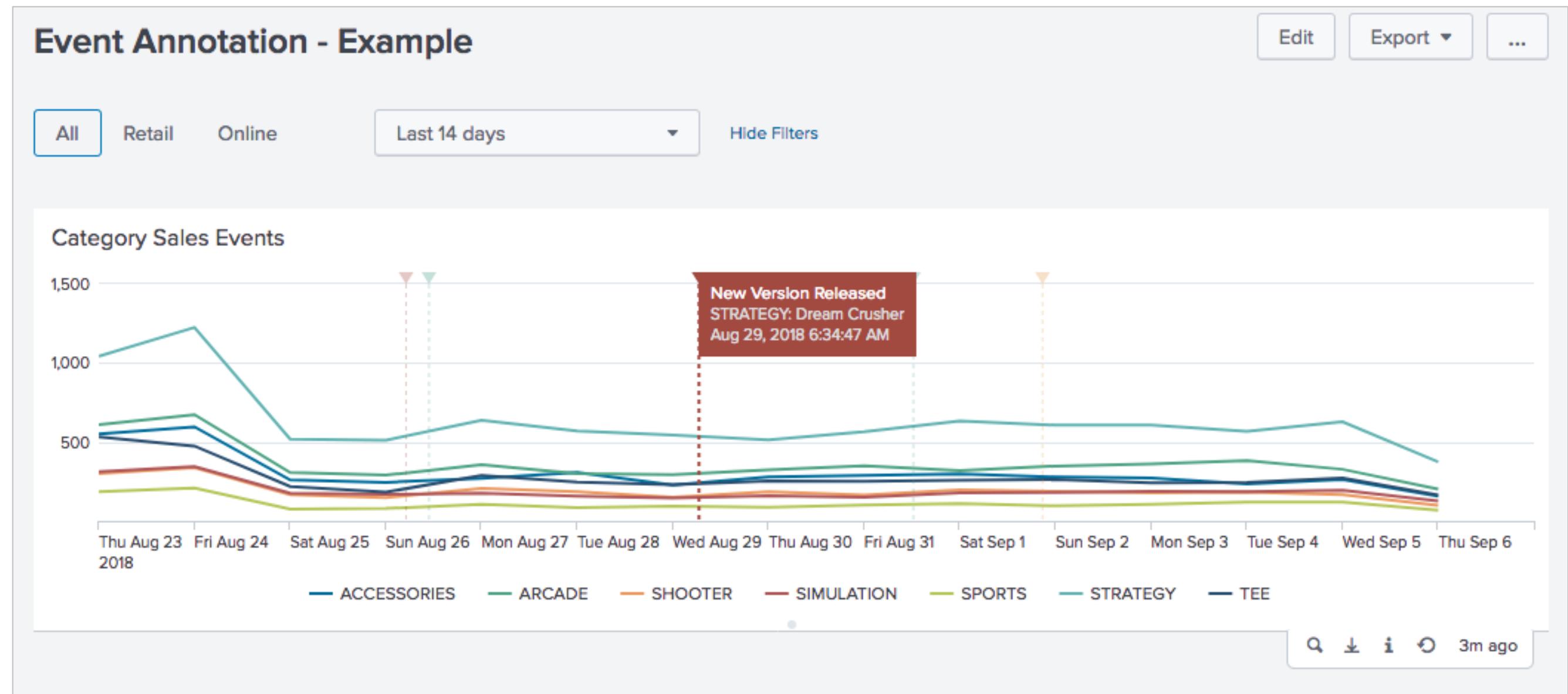
# Event Annotation – Example

- 1 `_time`: required
- 2 Search type: required
- 3 `annotation_label`:  
Field in your data containing  
the text to display
- 4 `annotation_category`:  
Field in your data to group  
annotation events by
- 5 `annotation_color`:  
Assign a color to an  
annotation event using either  
HEX or RGB notation

```
...
<chart>
<search>
1 <query>$sales_type_tok$ categoryId!=NULL
| timechart count by categoryId</query>
<earliest>$time_tok.earliest$</earliest>
<latest>$time_tok.latest$</latest>
<sampleRatio>1</sampleRatio>
</search>
2 <search type="annotation">
3 <query>index="sales" sourcetype="bcg_sale_dates"
| eval annotation_label = message
4 | eval annotation_category = Sale_Category
</query>
<earliest>$time_tok.earliest$</earliest>
<latest>$time_tok.latest$</latest>
</search>
5 <option name="charting.annotation.categoryColors">
{"ARCADE": "0xff3300", "SIMULATION": "0xff9900",
"STRATEGY": "0xff3300", "TEE": "0xff9900",
"SPORTS": "0xff3300"}
</option>
...

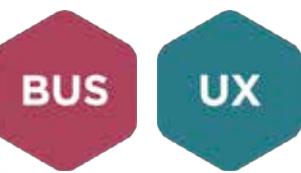
```

# Event Annotation – Example (cont.)

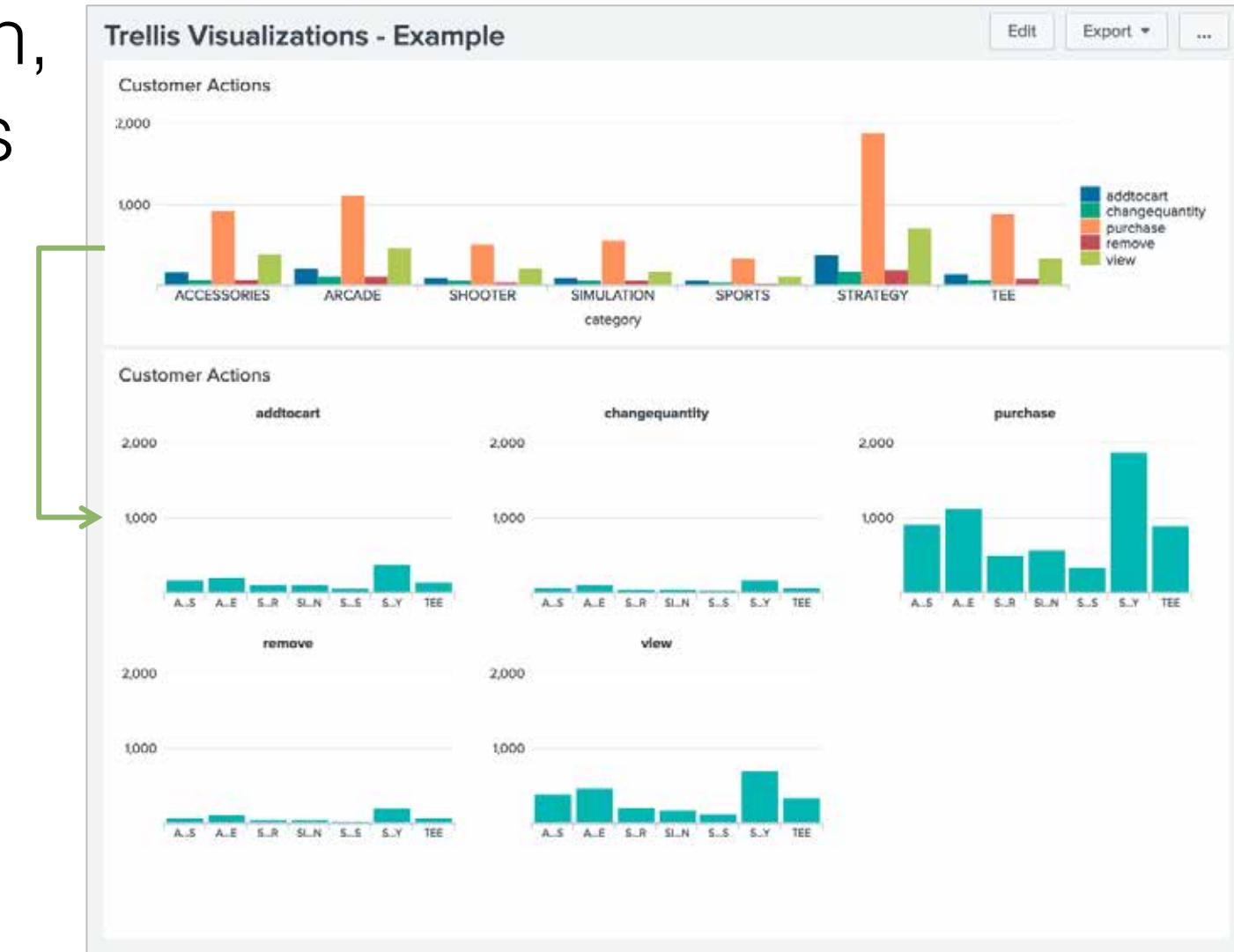


Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Trellis Visualizations



- Multiple instances of a visualization, where each instance shows values for just one category
- Driven by one query
- Split search results by fields or aggregations and visualize each field value separately



Note



Trellis layout is not available for tables or cluster maps.

# Trellis Visualizations (cont.)

1

2

3

4

Customer Actions

No title

2,000

1,000

0

category

ACCESSORIES ARCADE SHOOTER SIMULATION SPORTS STRATEGY TEE

addtocart changequantity purchase remove view

Customer Actions

No title

2,000

1,000

0

addtocart changequantity purchase remove view

A.S A.E S.R S.N S.S S.Y TEE

Customer Actions

No title

2,000

1,000

0

purchase

A.S A.E S.R S.N S.S S.Y TEE

Customer Actions

No title

2,000

1,000

0

remove

A.S A.E S.R S.N S.S S.Y TEE

Customer Actions

No title

2,000

1,000

0

view

A.S A.E S.R S.N S.S S.Y TEE

Customer Actions

No title

2,000

1,000

0

purchase

A.S A.E S.R S.N S.S S.Y TEE

Customer Actions

No title

2,000

1,000

0

remove

A.S A.E S.R S.N S.S S.Y TEE

Customer Actions

No title

2,000

1,000

0

view

A.S A.E S.R S.N S.S S.Y TEE

...<panel><title>Customer Actions</title><chart><search><query>sourcetype=access\_combined action!=NULL categoryId!=NULL | rename categoryId as "category" | chart count by category, action</query><earliest>-30d@d</earliest><latest>now</latest><sampleRatio>1</sampleRatio></search><option name="charting.axisTitleX.visibility">collapsed</option><option name="charting.axisTitleY.visibility">collapsed</option><option name="charting.axisTitleY2.visibility">collapsed</option><option name="charting.chart">column</option><option name="charting.drilldown">none</option><option name="charting.legend.placement">none</option><option name="height">627</option><option name="trellis.enabled">1</option><option name="trellis.scales.shared">1</option><option name="trellis.splitBy">action</option></chart></panel>...

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Table Formats



- Set color and number format by column
- Color data
  - Scale, range or value
- Format numbers
  - Currency symbols and thousands separators

Color Formatting

The screenshot shows a 'Color' dropdown set to 'None'. Below it are three sections: 'Scale' (with a preview of 0, 1, 3, 5, 7), 'Ranges' (with a preview of 0, 1, 6, 7, 9), and 'Values' (with a preview of a, b, a, b, d). A green arrow points from the 'Color Formatting' callout to the top right corner of the dialog.

Number Formatting

The screenshot shows the 'Number Formatting' tab selected. It includes fields for 'Color' (set to 'Enabled'), 'Precision' (set to '0.00'), 'Use Thousand Separators' (set to 'Yes'), 'Unit' (set to '\$'), and 'Unit Position' (set to 'Before'). A green arrow points from the 'Number Formatting' callout to the top right corner of the dialog.

Note

Table formats are discussed in detail in the Splunk Fundamentals 1 course.

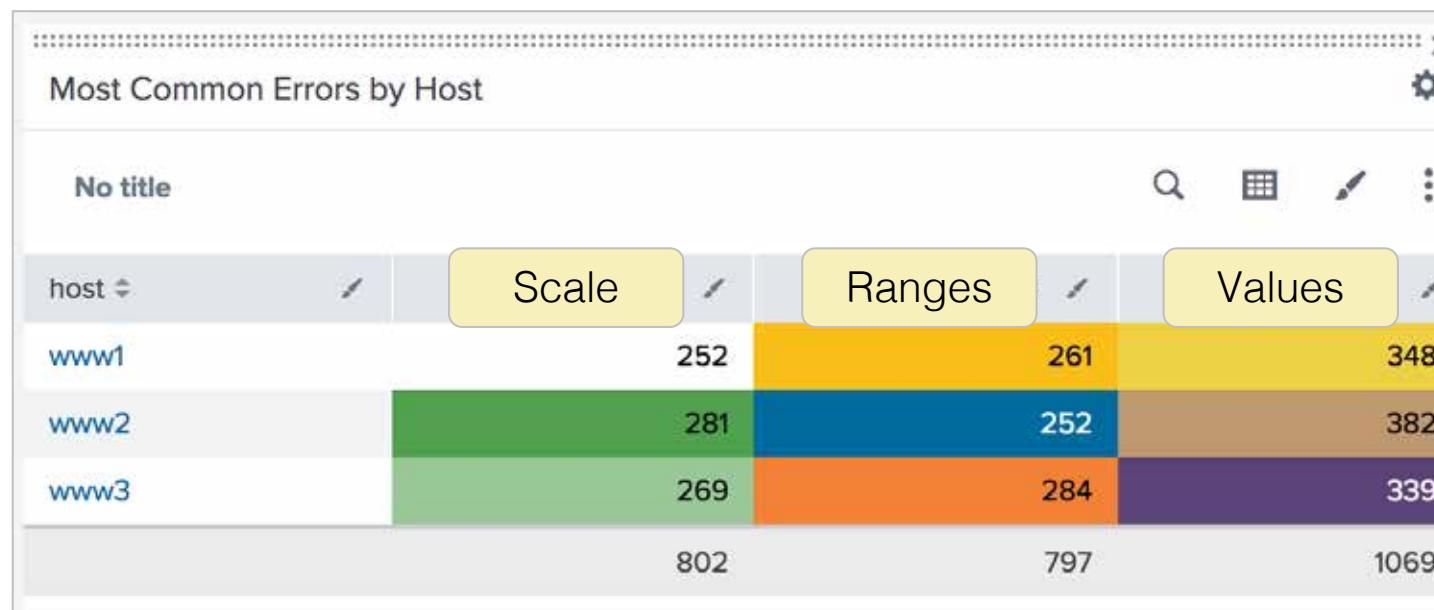
Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Table Formats (cont.)

- Cell colors change based on the scale, range or values you define:
  - **None**: no color coding (default)
  - **Scale**: numeric data
  - **Ranges**: numeric data
  - **Values**: numeric and non-numeric

The image displays three separate configuration panels from the Splunk interface:

- Color:** Shows a "Ranges" tab with two defined ranges: one from 250 to 250 (green) and another from 250 to 260 (blue). It also shows a "Number Formatting" section.
- Scale:** Shows a "Scale" tab with a color palette, "Presets" dropdown set to green, and controls for "Minimum" (Lowest Value), "Midpoint" (None), and "Maximum" (Highest Value).
- Values:** Shows a "Values" tab with "Automatic" selected, a "Number Formatting" section, and a "Cell value is" field with a green color swatch and a "+ Add Rule" button.



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Panel Link Buttons



Property	Type	Description
link.visible	Boolean	Show link buttons at bottom of panel
refresh.time.visible	Boolean	Display the Refresh Time
refresh.link.visible	Boolean	Show the Refresh Link
link.inspectSearch.visible	Boolean	Show the Inspect button
link.exportResults.visible	Boolean	Show the Export Results button
link.openSearch.visible	Boolean	Show the Open Search button
- link.openSearch.search	Search String	Alternative search to use for the Open in Search button
- link.openSearch.text	Text	Label to use for the Open in Search button
- link.openSearch.viewTarget	View Name	Target view for the Open in Search button

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Panel Link Buttons – Example

The image shows two Splunk dashboards side-by-side. The left dashboard is titled "Total Vendor Sales" and displays a large value of "42,897" with a timestamp of "Last 30 Days". Below the value is a button labeled "Go to BCG Sales Dashboard". The right dashboard is titled "BCG Sales Dashboard" and contains a pie chart titled "All Sales by Product" showing sales distribution across various products. To the right of the pie chart is a table titled "Sales Totals by Product" listing products and their sales amounts. A green callout box highlights the code for the panel link buttons, which is displayed in a box below the dashboards.

```
...  
    <option name="link.exportResults.visible">0</option>  
    <option name="link.inspectSearch.visible">0</option>  
    <option name="refresh.link.visible">0</option>  
    <option name="link.openSearch.text">Go to BCG Sales Dashboard</option>  
    <option name="link.openSearch.viewTarget">bcg_sales</option>  
    <option name="underLabel">Last 30 Days</option>  
  </single>  
</panel>  
...
```

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Search Refresh Indicator



Search Refresh - Example

None - Background Search with No Progress Bar      Progress Bar      Default      Preview and Progress Bar

626,935      626,935

Waiting for data...

Edit search

1      42          

Edit Search

Title: Preview and Progress Bar

Search String: sourcetype=vendor\_sales | stats count

Run Search

Time Range: Use time picker      Last 30 days

Auto Refresh Delay : 5 minutes

Refresh Indicator:   
None  
Background Search with No Progress Bar  
**Progress bar**   
Background Search with Progress Bar  
Preview and progress bar  
Preview Events with Progress Bar

Report      Apply

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Auto-Refresh



- Inline and reports only
- Enabling for a report or base search requires editing the XML
  - Post process searches will automatically refresh when their base search is refreshed

```
...
<panel>
  <single>
    <title>All Vendor Sales</title>
    <search>
      <query>sourcetype=vendor_sales | stats count</query>
      <earliest>-30d@d</earliest>
      <latest>now</latest>
      <sampleRatio>1</sampleRatio>
      <refresh>10m</refresh>
      <refreshType>delay</refreshType>
    </search>
  ...

```

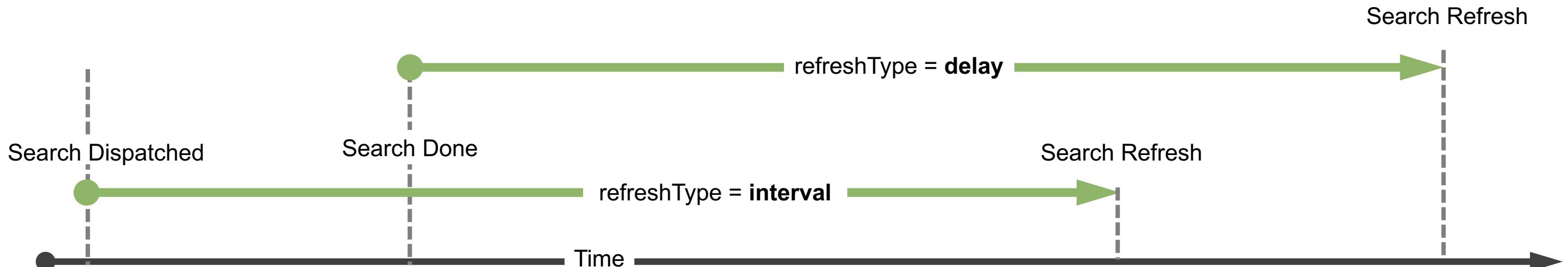
The screenshot shows the 'Edit Search' interface for a search titled 'All Vendor Sales'. The search string is 'sourcetype=vendor\_sales | stats count'. The time range is set to 'Last 30 days'. The 'Auto Refresh Delay' dropdown is open, showing options: 'No auto refresh', '30 seconds', '1 minute', '2 minutes', '5 minutes', '10 minutes' (which is selected), and 'Custom'. A green 'Apply' button is visible at the bottom right of the dropdown.

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Auto-Refresh (cont.)

- **refresh**: amount of time between refreshes
  - Default: do not refresh
- **refreshType**: point from which the refresh time is counted
  - delay: start counting down when search is done (default)
  - interval: start counting when search is dispatched

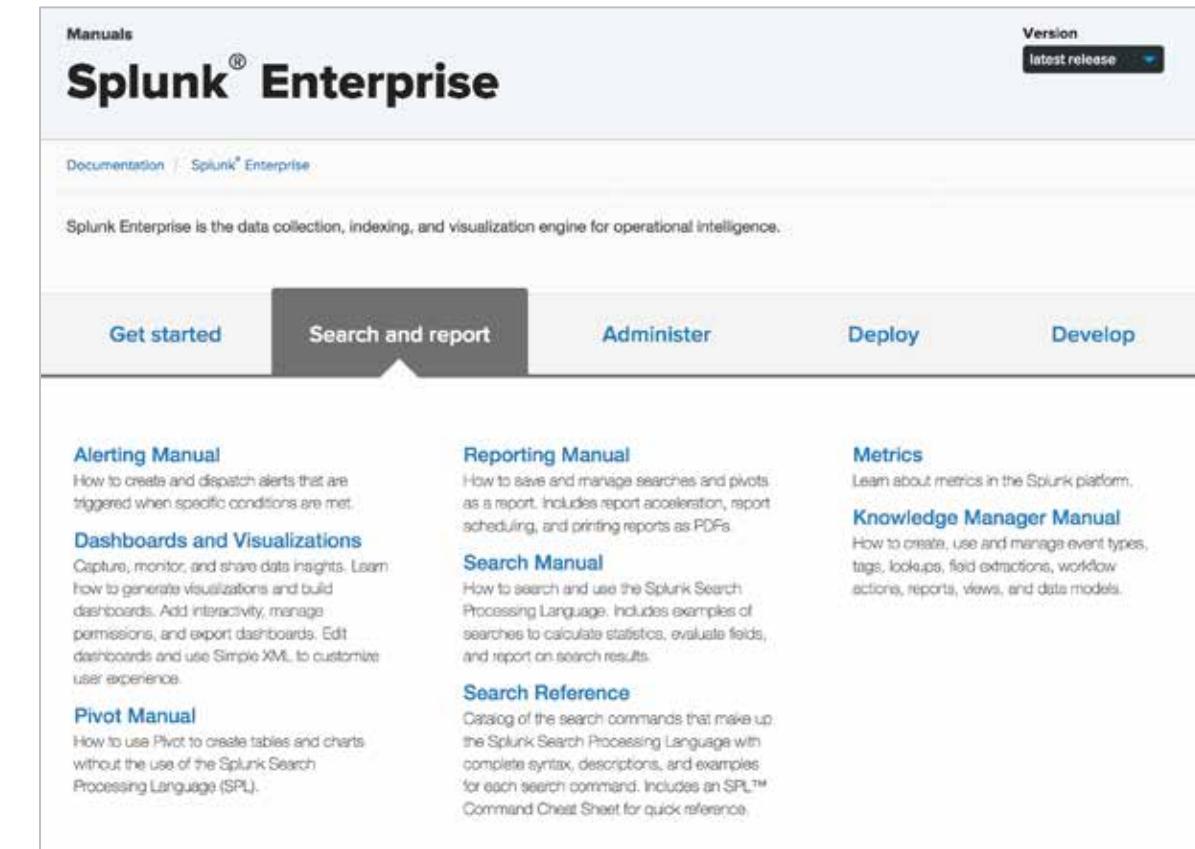
```
...
<search>
  <query>sourcetype=vendor_sales | stats count</query>
  <earliest>-30d@d</earliest>
  <latest>now</latest>
  <sampleRatio>1</sampleRatio>
  <refresh>10m</refresh>
  <refreshType>delay</refreshType>
</search>
...
...
```



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Useful References

- Simple XML Reference  
[docs.splunk.com/Documentation/Splunk/latest/Viz/PanelreferenceforSimplifiedXML](https://docs.splunk.com/Documentation/Splunk/latest/Viz/PanelreferenceforSimplifiedXML)
- Visualization Reference  
[docs.splunk.com/Documentation/Splunk/latest/Viz/Visualizationreference](https://docs.splunk.com/Documentation/Splunk/latest/Viz/Visualizationreference)
- Chart Configuration Reference  
[docs.splunk.com/Documentation/Splunk/latest/Viz/ChartConfigurationReference](https://docs.splunk.com/Documentation/Splunk/latest/Viz/ChartConfigurationReference)
- Table Visualizations  
[docs.splunk.com/Documentation/Splunk/latest/Viz/TableFormats](https://docs.splunk.com/Documentation/Splunk/latest/Viz/TableFormats)



The screenshot shows the Splunk Enterprise Documentation homepage. At the top right, there is a "Version" dropdown set to "Latest release". The main title is "Splunk® Enterprise" with a "Manuals" link above it. Below the title, it says "Splunk Enterprise is the data collection, indexing, and visualization engine for operational intelligence." A navigation bar at the bottom includes links for "Get started", "Search and report" (which is highlighted in dark grey), "Administer", "Deploy", and "Develop". On the left, there's a sidebar with links for "Alerting Manual", "Dashboards and Visualizations", "Search Manual", and "Pivot Manual". On the right, there are links for "Reporting Manual", "Metrics", and "Knowledge Manager Manual".

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

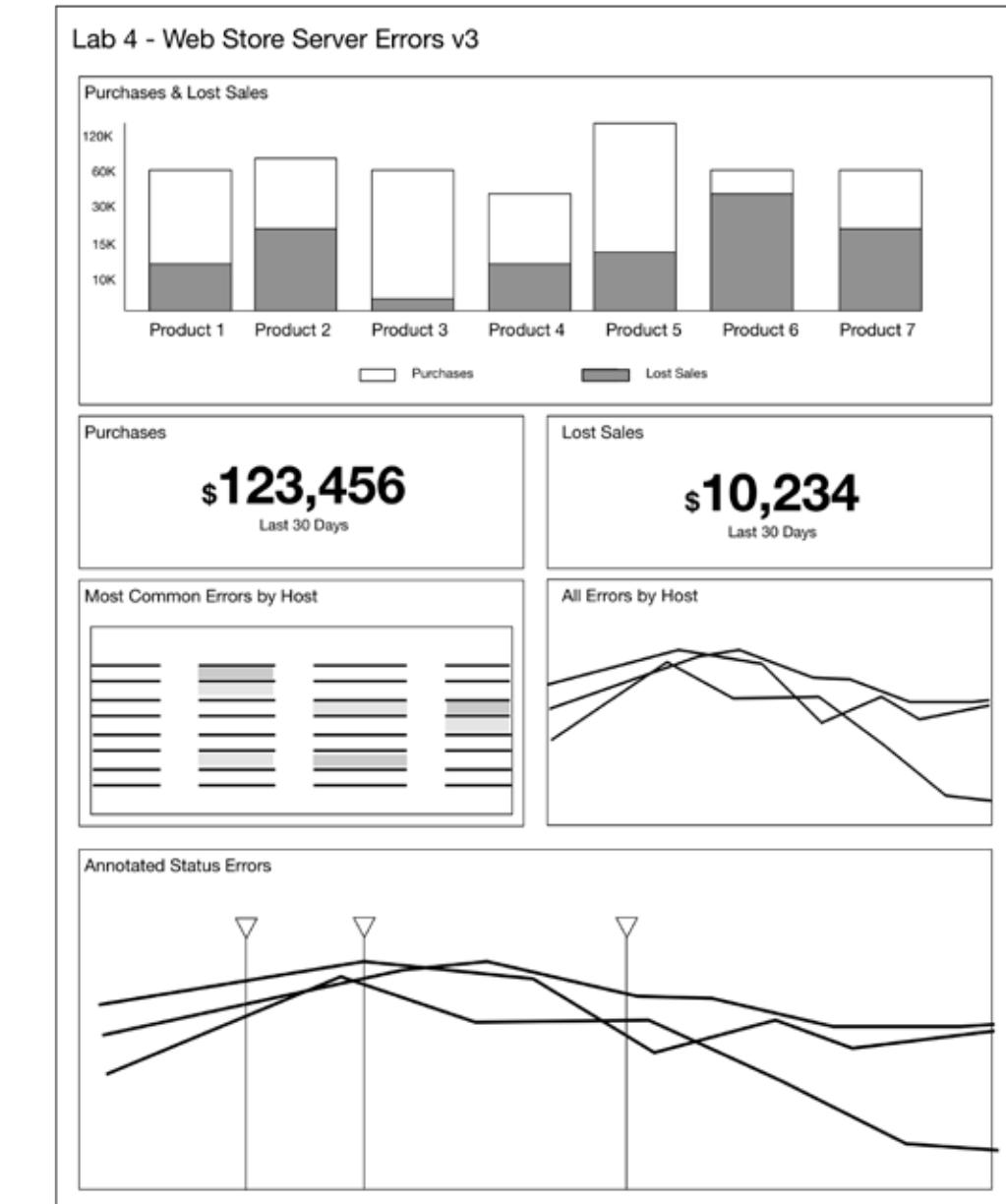
# Lab 4 – Customizing Dashboards

Time: 30 minutes

Scenario: Stakeholders have approved the dashboard with some changes. They'd like to use the company's brand colors, hide panel search controls, set refresh time, have the table cell colors match value severity, and have the map display bubbles instead of pies.

## Tasks:

- Customize chart colors
- Hide search controls
- Set panel refresh indicator
- Set panel refresh time
- Add column summaries and cell colors
- Add event annotations



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Module 5: Adding Drilldowns

Generated for Matt Brown ([mbrown@idbny.com](mailto:mbrown@idbny.com)) (C) Splunk Inc, not for distribution

# Module Objectives

---

- Describe four types of drilldowns
- Identify types of predefined drilldown tokens
- Create a dynamic drilldown
- Explain how to create a multiple fields dynamic drilldown

# Drilldowns



- Type of event handler
  - Default: event and visualization
  - Custom: Drilldown Editor and XML Editor
- Event drilldown
  - Click an event to see a pop-up menu with options
- Visualization drilldown
  - Clicking on a visualization redirects you to search view

A screenshot of a Splunk search results page showing three events. The third event is selected, and a context menu is open with options: 'Add to search' (highlighted), 'Exclude from search', and 'New search'. A yellow callout box labeled 'Event Drilldown' points to the menu.

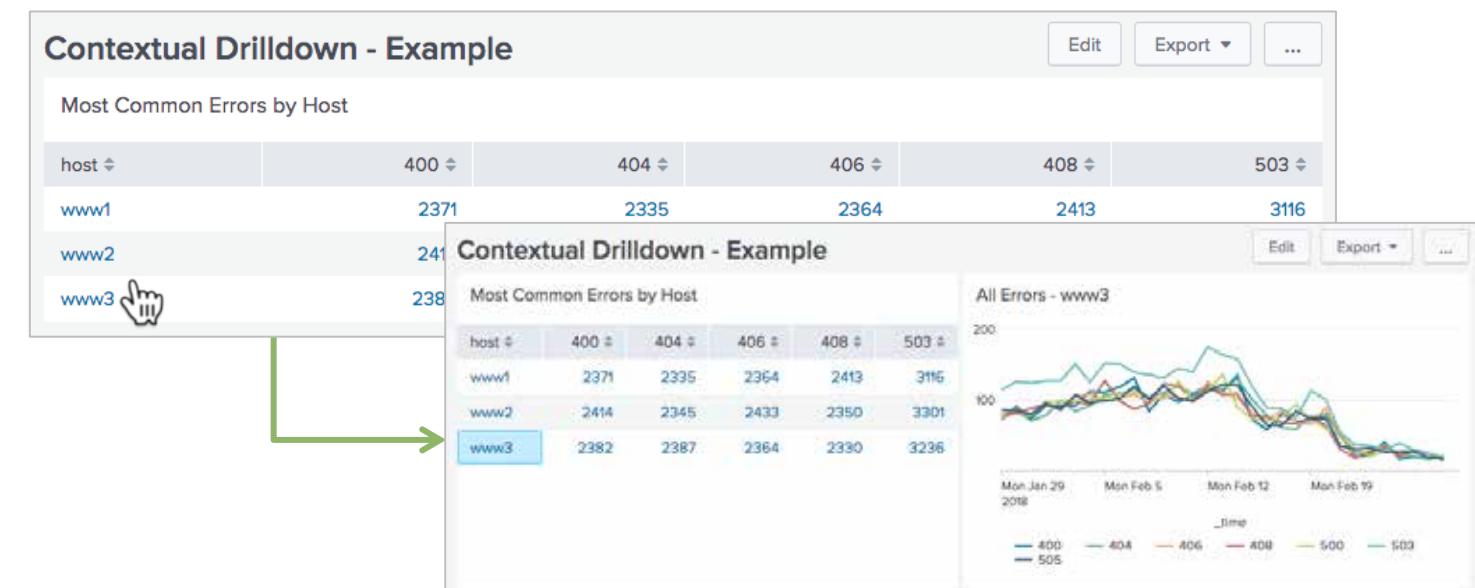
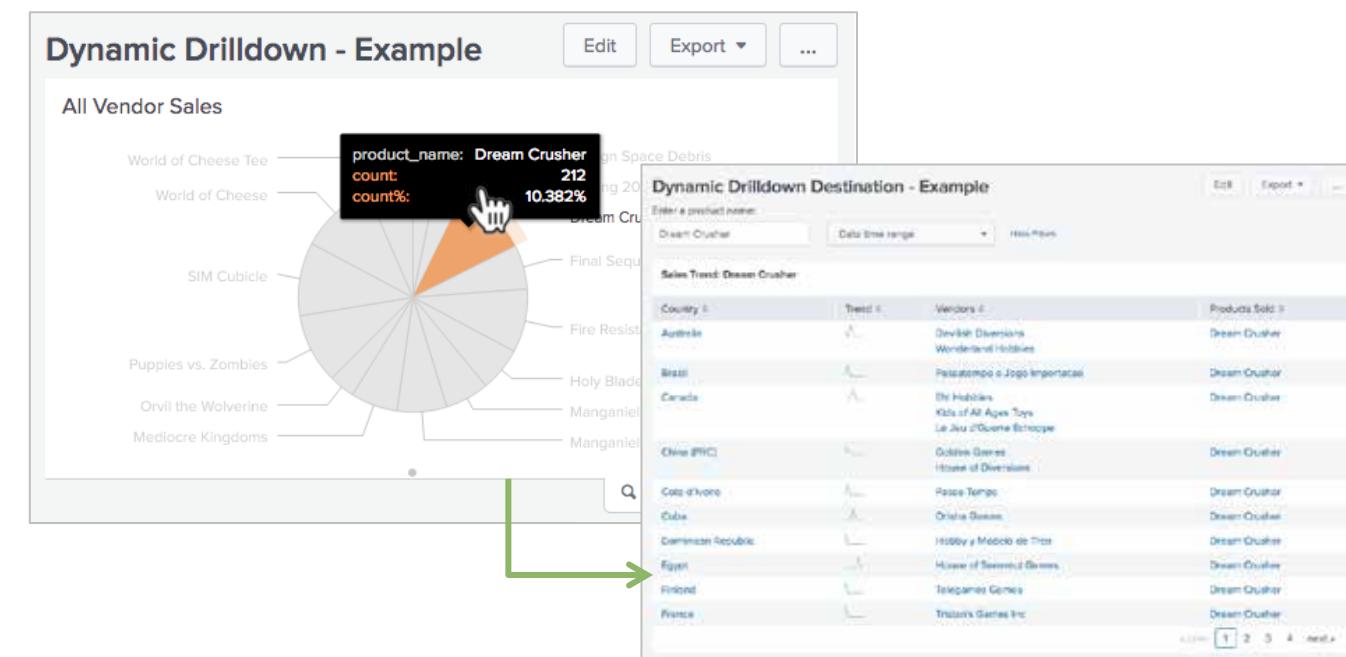
A screenshot of a Splunk search interface. On the left, a table titled 'Top Vendors' lists various vendors with their counts. An arrow points from the 'Atlanta Hobby Warehouse' row to a search results page on the right. The search results page shows a histogram for 'sourcetype=vendor\_sales' and 'Vendor="Atlanta Hobby Warehouse"'. A yellow callout box labeled 'Visualization Drilldown' points to the search results page.

Note

Event handlers are covered in Module 6.

# Drilldowns (cont.)

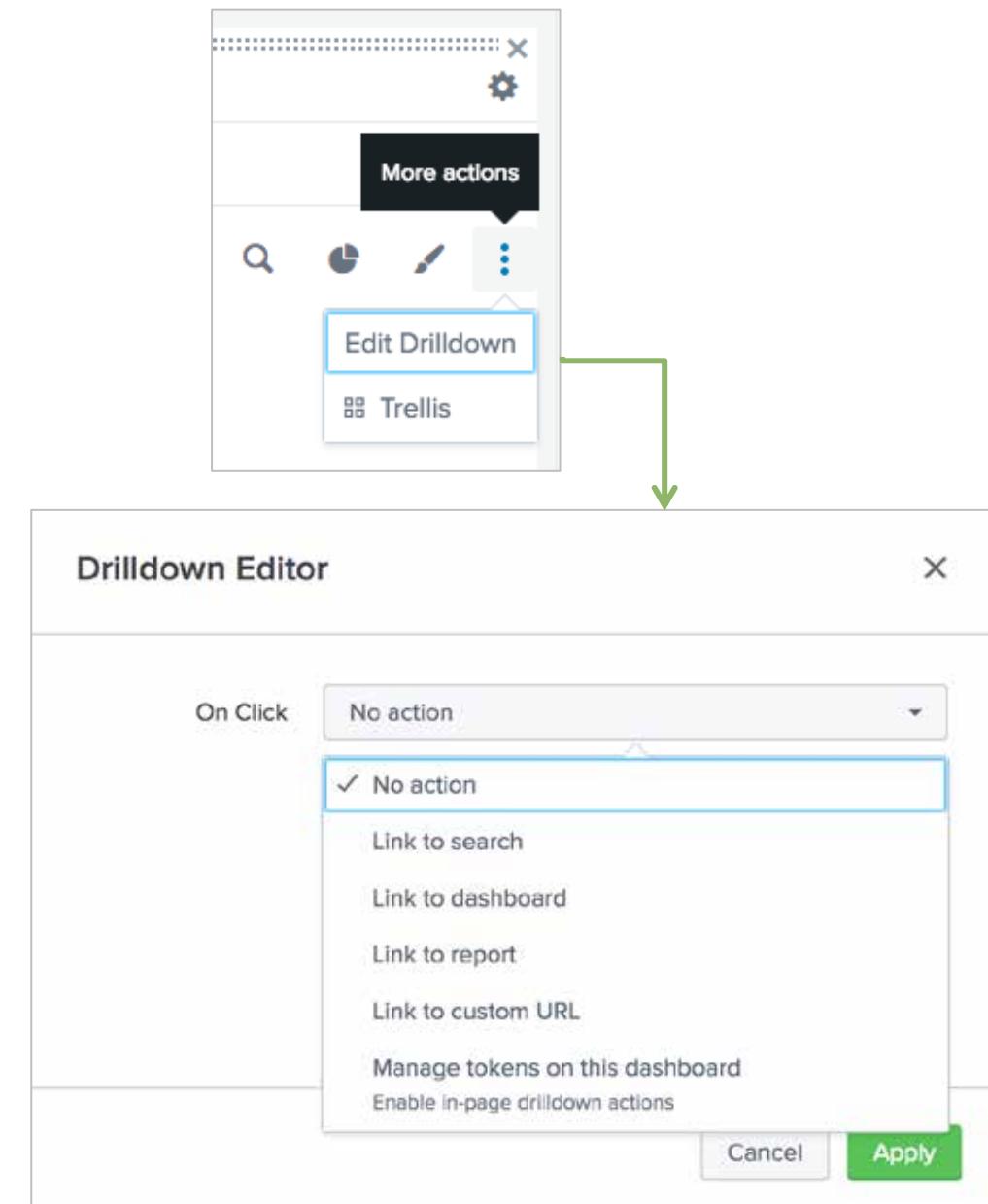
- Dynamic drilldowns
  - Pass a value from a user click to another panel, form, dashboard or external page
- Contextual drilldown
  - Dashboard elements listen for token values to be updated and trigger actions in response



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Drilldown Editor

- Use to configure a drilldown action
  - Dynamic and contextual drilldowns
- Specify a path to a destination
- Use <set>, <eval>, and <unset> to update token values
- Adds token filters automatically



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Drilldown Editor – Dynamic Drilldown Example

The following code snippets are extracted from the dashboard XML and the Drilldown Editor configuration:

```
<panel>
    <title>All Vendor Sales</title>
    <chart>
        <search>
            <query>sourcetype=vendor_sales | chart count by product_name</query>
            <earliest>-7d@d</earliest>
            <latest>now</latest>
            <sampleRatio>1</sampleRatio>
            <refresh>5m</refresh>
            <refreshType>delay</refreshType>
        </search>
        <option name="charting.chart">pie</option>
        <option name="charting.drilldown">all</option>
        <option name="refresh.display">progressbar</option>
        <drilldown>
            <link target="_blank">/app/sales/dynamic_drilldown_destination?form.product_name_tok=$click.value$&earliest=$earliest$&latest=$latest$</link>
        </drilldown>
    </chart>
</panel>
```

Drilldown Editor Configuration (Step 1):

- On Click: Link to dashboard
- App: No action
- Dashboard: Link to search
- Advanced: Link to dashboard (selected)

Drilldown Editor Configuration (Step 2):

- On Click: Link to dashboard
- App: Buttercup Games - Sales
- Dashboard: Sales - Drilldown Destination
- Advanced: Open in new tab
- Parameters:
  - product\_name\_tok = \$click.name\$
  - + Add New: \$click.value\$

Drilldown Editor Configuration (Step 3):

- On Click: Link to dashboard
- App: Buttercup Games - Sales
- Dashboard: Sales - Drilldown Destination
- Advanced: Open in new tab
- Parameters:
  - product\_name\_tok = \$click.value\$
  - earliest = \$earliest\$
  - latest = \$latest\$
  - + Add New: \$click.value2\$

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Drilldowns – Predefined Tokens

- Predefined tokens capture information when a user clicks a visualization
- Use different tokens to capture a click location or related data
- Tokens available depend on the visualization type

Table & Event	Single Value	Map	Chart
<p>\$click.name\$ Leftmost field (column) name in the table.</p> <p>\$click.value\$ Leftmost field (column) value in the clicked table row.</p> <p>\$click.name2\$ Clicked field (column) name.</p> <p>\$click.value2\$ Clicked field (column) value. Captures the specific table cell value that users click.</p> <p>\$row.&lt;fieldname&gt;\$ Access any field (column) value from the clicked table row.</p> <p>\$earliest\$ Earliest time of the clicked table row, or if not applicable, the earliest time of the search.</p> <p>\$latest\$ Latest time of the clicked table row, or if not applicable, the latest time of the search.</p>	<p>\$click.name\$ Name of the field that the single value represents.</p> <p>\$click.value\$ Field value that the single value represents.</p> <p>\$click.name2\$ Same as click.name.</p> <p>\$click.value2\$ Same as click.value.</p> <p>\$row.&lt;fieldname&gt;\$ Access any field value from the Statistics table row for the single value.</p> <p>\$earliest\$ Earliest time of the search driving the single value visualization.</p> <p>\$latest\$ Latest time of the search driving the single value visualization.</p> <p>\$trellis.name\$ Trellis layout split field name.</p> <p>\$trellis.value\$ Trellis layout split field value for the clicked segment.</p> <p>\$trellis.split.&lt;fieldname&gt;\$ Trellis layout aggregation or field value for the clicked visualization segment.</p>	<p>\$click.name\$ Field name for the clicked location. If multiple fields are associated with the location, uses the first field.</p> <p>\$click.value\$ Field value for the clicked location. If multiple fields are associated with the location, uses the first field.</p> <p>\$click.name2\$ Same as click.name.</p> <p>\$click.value2\$ Same as click.value.</p> <p>\$click.lat.name\$ For cluster maps: latitude field name for the clicked location.</p> <p>\$click.lat.value\$ For cluster maps: latitude field value for the clicked location.</p> <p>\$click.lon.name\$ For cluster maps: longitude field name for the clicked location.</p> <p>\$click.lon.value\$ For cluster maps: longitude field value for the clicked location.</p> <p>\$click.bounds.\$ For cluster maps: south, west, north, or east outer boundary for the clicked location. For example, use \$click.bounds.south\$ to get the eastern outer boundary.</p> <p>\$row.&lt;fieldname&gt;\$ Access field values related to the clicked location. Check the Statistics tab for available fields.</p> <p>\$earliest\$ Earliest time for the search generating the map.</p> <p>\$latest\$ Latest time for the search generating the map.</p> <p>\$trellis.name\$ For choropleth maps: trellis layout split field name.</p> <p>\$trellis.value\$ For choropleth maps: trellis layout split field value for the clicked segment.</p> <p>\$trellis.split.&lt;fieldname&gt;\$ For choropleth maps: trellis layout aggregation or field value for the clicked visualization segment.</p>	<p>\$click.name\$ X-axis field or category name for the clicked location. Not available if the user clicks the chart legend.</p> <p>\$click.value\$ X-axis field or category value for the clicked location. Not available if the user clicks the chart legend.</p> <p>\$click.name2\$ Y-axis field or series name for the clicked location. Not available if the user clicks the chart legend.</p> <p>\$click.value2\$ Y-axis field or series value for the clicked location. Not available if the user clicks the chart legend.</p> <p>\$row.&lt;fieldname&gt;\$ Access any x-axis field value corresponding to the clicked location x-axis. Not available if the user clicks the chart legend.</p> <p>\$earliest\$ Earliest time for the clicked chart segment. If not applicable, uses the earliest time for the search.</p> <p>\$latest\$ Latest time for the clicked chart segment. If not applicable, uses the latest time for the search.</p> <p>\$trellis.name\$ Trellis layout split field name.</p> <p>\$trellis.value\$ Trellis layout split field value for the clicked segment.</p> <p>\$trellis.split.&lt;fieldname&gt;\$ Trellis layout aggregation or field value for the clicked visualization segment.</p>

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Dynamic Drilldown – Example 1

Table row: Use the `$row.field_name$` token to pass a value from a row click

Dynamic Drilldown - Example 1

All Sales by Vendor - Last 7 Days

product_name	Vendor	count	percent
Fire Resistance Suit of Provolone	Ahimsa Games	3	2.083333
World of Cheese	Beach Games	3	1.604278
Fire Resistance Suit of Provolone	Beauty Games	3	2.083333

```
...
<panel>
  <title>All Sales by Vendor - Last 7 Days</title>
  <table>
    <search>
      <query>sourcetype=vendor_sales product_name="*" | top Vendor by product_name | sort Vendor</query>
      <earliest>-7d@d</earliest>
      <latest>now</latest>
      <sampleRatio>1</sampleRatio>
    </search>
    <option name="count">10</option>
    <option name="drilldown">cell</option>
    <option name="wrap">true</option>
    <drilldown>
      <link target="_blank">/app/sales/dynamic_drilldown_destination?form.product_name_tok=$row.product_name$&earliest=$earliest$&latest=$latest$</link>
    </drilldown>
  </table>
</panel>
```

Drilldown Editor

On Click: Link to dashboard

App: Buttercup Games - Sales

Dashboard: Sales - Drilldown Destination

Open in new tab

Advanced

Parameters:

- form.product\_name = \$row.product\_name\$
- earliest = \$earliest\$
- latest = \$latest\$

+ Add New

Use parameters to set token values in the target dashboard. For example, form.host=\$click.value2\$ or host=\$row.host\$. Learn more.

Preview URL: /app/sales/dynamic\_drilldown\_destination?form.product\_name\_tok=\$row.product\_name\$&earliest=\$earliest\$&latest=\$latest\$

Cancel Apply

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

101

splunk® listen to your data®

Creating Dashboards

Copyright © 2018 Splunk, Inc. All rights reserved | 30 August 2019

# Dynamic Drilldown – Example 2

Chart: Use the `$click.value$` token to pass a value from a click

The diagram illustrates the configuration of a dynamic drilldown in Splunk. It shows a chart titled "Top Product Sales - Last 7 Days" with a selected segment for "World of Cheese". Below the chart is the corresponding XML code. To the right is the "Drilldown Editor" window.

**Chart:** Top Product Sales - Last 7 Days

**Drilldown Editor:**

1. On Click: Link to dashboard
2. App: Buttercup Games - Sales
3. Dashboard: Sales - Drilldown Destination
4. Advanced parameters:
  - form.product\_name = \$click.value\$
  - earliest = \$earliest\$
  - latest = \$latest\$

**XML Code:**

```
<panel>
  <title>Top Product Sales - Last 7 Days</title>
  <chart>
    <search>
      <query>sourcetype=vendor_sales | top product_name</query>
      <earliest>-7d@d</earliest>
      <latest>now</latest>
      <sampleRatio>1</sampleRatio>
    </search>
    ...
    <drilldown>
      <link target="_blank">/app/sales/dynamic_drilldown_destination?form.product_name_tok=$click.value$&earliest=$earliest$&latest=$latest$</link>
    </drilldown>
  </chart>
</panel>
```

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Drilldown Destination Form

Add the token to the destination form's input and search

```
<form>
  <label>Sales - Drilldown Destination</label>
  <fieldset autoRun="true" submitButton="false">
    <input type="text" searchWhenChanged="true" token="product_name_tok">
      <label>Enter a product name:</label>
      <default>*</default>
    </input>
    <input type="time" searchWhenChanged="true">
      <label></label>
      <default>
        <earliest>$earliest$</earliest>
        <latest>$latest$</latest>
      </default>
    </input>
  </fieldset>
  <row>
    <panel>
      <table>
        <title>Sales Trend: $product_name_tok$</title>
        <search>
          <query>sourcetype=vendor_sales product_name=$product_name_tok$ | stats sparkline(count) as Trend values(Vendor) as "Vendors" by VendorCountry | rename VendorCountry as "Country" | sort Country</query>
          <earliest>$earliest$</earliest>
          <latest>$latest$</latest>
        </search>
        ...
      </table>
    </panel>
  </row>
</form>
```

your custom token from the source dashboard

your custom token from the source dashboard plus a token filter to add quotes in the search

Sales - Drilldown Destination

Enter a product name: World of Cheese Date time range Hide Filters

Sales Trend: World of Cheese

Country	Trend	Vendors
Andorra	↙	EuroToys Emporium
Argentina	↙	Juegos de Alfredo
Austria	↙	Spa und Spiele
Belgium	↖	Anneaux du Temps
Brazil	↖	Casa de Pasatiempos y Juegos Passatempo e Jogo Importacao
Canada	↘	Maple Leaves Hobbies & Toys Model Railroading & Hobbies Sunshine Games Ye Olde Game Shoppe
China (PRC)	↗	Golden Games House of Diversions
Colombia	↖	Hobby y Modelo de Tren
Cyprus	↙	Green Line Games
France	↙	Centre du Hobby

« prev 1 2 3 next »

## Note

Use a token filter in the destination form since best practice is for it to include an input — which means a token; a token on both the drilldown and the destination will not work.

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Dynamic Drilldown – Multiple Fields

Use the `condition` element with `field=source_field_name` and multiple link tags to make multiple fields clickable

Dynamic Drilldown - Multiple Fields Example

Top Sales by Vendor

Vendor	product_name
Playtime Game & Hobby Shop	Puppies vs. Zombies
Playtime Game & Hobby Shop	Dream Crusher
Playtime Game & Hobby Shop	World of Cheese
Playtime Game & Hobby Shop	Fire Resistance Suit of I
Playtime Game & Hobby Shop	World of Cheese Tee
Playtime Game & Hobby Shop	Holy Blade of Gouda
Playtime Game & Hobby Shop	SIM Cubicle
House of Diversions	Dream Crusher
EuroToys Emporium	World of Cheese Tee
EuroToys Emporium	Manganiello Bros. Tee

```
<drilldown>
<condition field=source_field_name1>
  <link>/relative_path/view_id?form.target_token1=$row.source_field_name1$</link>
</condition>
<drilldown>

<table>
  <search ref="Top Sales by Vendor and Product"></search>
  <drilldown>
    <condition field="Vendor">
      <link target="_blank">/app/sales/sales_drilldown_dest?form.vendor_tok=$row.Vendor$</link>
    </condition>
    <condition field="product_name">
      <link target="_blank">/app/sales/sales_drilldown_dest?form.product_name_tok=$row.product_name$</link>
    </condition>
  </drilldown>
</table>
</panel>
</row>
</dashboard>
```

## Note

Multiple field dynamic drilldown is not available in the drilldown editor. It requires editing the XML.

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Drilldown Destination Form – Multiple Fields

Include an input for each token being passed to the destination form

Drilldown Destination - Example 2

Enter a vendor name: Enter a product name:

Puppies vs. Zombies All time

Sales Trend

Country	Trend	Vendors
Argentina		San Martin Hobby Club
Armenia		EuroToys Emporium
Australia		Devilish Diversions Geppetto's Toys
Austria		Spa und Spiele
Belgium		Anneaux du Temps
Brazil		Casa de Pasatiempos y Juegos Passatempo e Jogo Importacao
Canada		Games People Play Kids of All Ages Toys
China (PRC)		Golden Games House of Diversions
Colombia		Hobby y Modelo de Tren
Czech Republic		EuroToys Emporium

...

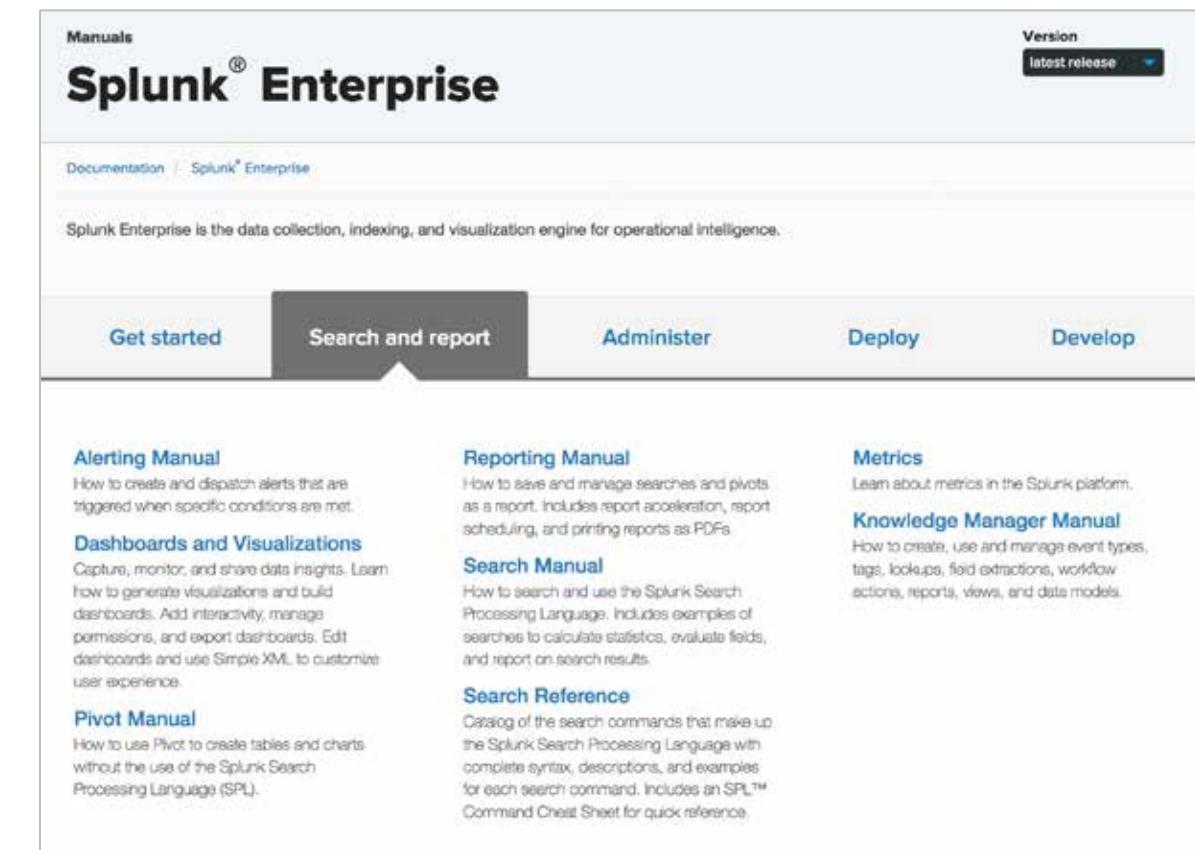
```
<fieldset autoRun="true" submitButton="false">
  <input type="text" searchWhenChanged="true" token="vendor_tok">
    <label>Enter a vendor name:</label>
    <default>*</default>
  </input>

  <input type="text" searchWhenChanged="true" token="product_name_tok">
    <label>Enter a product name:</label>
    <default>*</default>
  </input>
</fieldset>
<row>
<panel>
<table>
  <title>Sales Trend</title>
  <search>
    <query>sourcetype=vendor_sales product_name="$product_name_tok$" Vendor="$vendor_tok$"
      | stats sparkline(count) as Trend values(Vendor) as "Vendors" values(product_name) as
        "Products Sold" by VendorCountry
      | rename VendorCountry as "Country"
      | sort Country</query>
    <earliest>-7d@h</earliest>
    <latest>now</latest>
  </search>
  ...
</table>
</panel>
</row>
```

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Useful References

- Use Drilldown for Dashboard Interactivity  
[docs.splunk.com/Documentation/Splunk/latest/Viz/DrilldownIntro](https://docs.splunk.com/Documentation/Splunk/latest/Viz/DrilldownIntro)
- Drilldown Elements  
[docs.splunk.com/Documentation/Splunk/latest/Viz/PanelreferenceforSimplifiedXML#drilldown](https://docs.splunk.com/Documentation/Splunk/latest/Viz/PanelreferenceforSimplifiedXML#drilldown)
- Predefined Drilldown Tokens  
[docs.splunk.com/Documentation/Splunk/latest/Viz/PanelreferenceforSimplifiedXML#Predefined\\_drilldown\\_tokens](https://docs.splunk.com/Documentation/Splunk/latest/Viz/PanelreferenceforSimplifiedXML#Predefined_drilldown_tokens)



The screenshot shows the Splunk Enterprise Documentation homepage. At the top right, there is a "Version" dropdown set to "Latest release". The main title is "Splunk® Enterprise" with a "Manuals" link above it. Below the title, there's a sub-navigation bar with links for "Documentation" and "Splunk® Enterprise". A brief description states: "Splunk Enterprise is the data collection, indexing, and visualization engine for operational intelligence." Below this, there are five main navigation tabs: "Get started", "Search and report" (which is highlighted in dark grey), "Administer", "Deploy", and "Develop". To the right of these tabs, there are two columns of documentation links:

- Alerting Manual**: How to create and dispatch alerts that are triggered when specific conditions are met.
- Reporting Manual**: How to save and manage searches and pivots as a report. Includes report acceleration, report scheduling, and printing reports as PDFs.
- Dashboards and Visualizations**: Capture, monitor, and share data insights. Learn how to generate visualizations and build dashboards. Add interactivity, manage permissions, and export dashboards. Edit dashboards and use Simple XML to customize user experience.
- Search Manual**: How to search and use the Splunk Search Processing Language. Includes examples of searches to calculate statistics, evaluate fields, and report on search results.
- Pivot Manual**: How to use Pivot to create tables and charts without the use of the Splunk Search Processing Language (SPL).
- Search Reference**: Catalog of the search commands that make up the Splunk Search Processing Language with complete syntax, descriptions, and examples for each search command. Includes an SPL™ Command Cheat Sheet for quick reference.

# Lab 5 – Add a Dynamic Drilldown

Time: 25 minutes

Scenario: The sales team wants to add a dynamic drilldown from the Sales by Category panel to a form that displays sales trends by category

Tasks:

- Create a drilldown destination form
- Add text and time inputs
- Clone a form
- Create a dynamic drilldown



# Module 6: Adding Advanced Behaviors & Visualizations

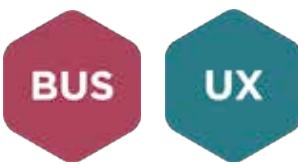
Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Module Objectives

---

- Identify types of event handlers
- Define event actions
- Define custom visualizations
- Use simple XML extensions

# Event Handlers

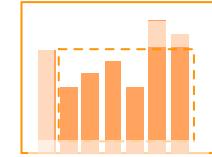


puppies vs. zom|

Form Input  
input value change



Search  
status of a search job



Visualization  
user selections and  
dynamic drilldowns

- Use event handlers with event actions
  - Tokens available to each handler vary
- Perform event actions based on user behavior or search job status:
  - Execute an eval statement
  - Link to another page
  - Set & unset tokens

# Event Handler – Example

- Contextual Drilldown
  - Table
    - Captures the value of the host field
    - Sets a token to make the chart visible
    - Populates the chart panel's search and title with the host value
  - Chart
    - Unsets the token to make the chart hidden

Most Common Errors by Host - Last 7 Days						
host	400	404	408	500	503	
www1	313	316	316	315	411	
www2	325	335	348	326	447	
www3	323	340	320	345	443	



Event Handler

```
...
<panel>
<table>
<search>
<query>sourcetype=access_combined status>399
| chart count by host, status limit=5 useother=f</query>
<earliest>-30d@d</earliest>
<latest>now</latest>
<sampleRatio>1</sampleRatio>
</search>
<drilldown>
<set token="host_errors_tok">$click.value$</set></drilldown>
</table>
</panel>
<panel>
<title>All Errors - $host_errors Tok$</title>
<chart depends="$host_errors Tok$">
<search>
<query>sourcetype=access* host="$host errors Tok$" status>399
| timechart count by status</query>
<earliest>-30d@d</earliest>
<latest>now</latest>
<sampleRatio>1</sampleRatio>
</search>
...
<drilldown>
<unset token="host_errors Tok$"></unset>
</drilldown>
</chart>
...

```

Event Action

Event Handler

Event Action

# Event Actions – Execute an Eval Statement

- <eval>
  - Execute an eval statement and put the results into a token

```
<eval token="myToken">tostring(round(field))</eval>
```

## Syntax by Event Handler

### Form Input

puppies vs. zom

```
<change>
<eval token="[token_name]">
```

### Search



```
<search>
<done | error | fail | cancelled | progress>
<eval token="[token_name]">
```

### Visualization



```
<[visualization]>
<drilldown>
<eval token="[token_name]">
<selection>
<eval token="[token_name]">
```

# Event Actions – Link to Another Page

- <link>
  - Specify a destination for a dynamic drilldown, selected input, or search
    - ▶ Dashboard    `<link>/app/myApp/myView</link>`
    - ▶ Form    `<link>/app/myApp/myView?form.token=$token$</link>`
    - ▶ URL    `<link>myURL?q=$token$</link>`

## Syntax by Event Handler

### Form Input

puppies vs. zom

```
<change>
```

```
<link>/app/appName/viewName
```

### Search



```
<search>
```

```
<done | error | fail | cancelled | progress>
<link>/app/appName/viewName
```

### Visualization



```
<selection>
```

```
<link>/app/appName/viewName
```

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Event Actions – Set & Unset Tokens

- **<set>**
  - Specify tokens for actions to take for specific inputs

```
<set token="myToken">$text$</set>
```

- **<unset>**
  - Remove a token that was previously set

```
<unset token="myToken"></unset>
```

## Syntax by Event Handler

Form Input

```
<change>
<set token="[token_name]">
<unset token="[token_name]">
```

Search 

```
<search>
<done | error | fail | cancelled | progress>
<set token="[token_name]">
<unset token="[token_name]">
```

Visualization 

```
<selection>
<set token="[token_name]">
<unset token="[token_name]">
```

# depends & rejects Attributes

- Show or hide content based on existence of a token
  - <row>, <panel>, <chart>, <table>, <events>, <input>, <search>
- Use with event handlers, drilldowns, condition element
- Can use multiple tokens, separated by commas
- depends: hide by default, show when token exists

```
<panel depends="$myPanel$"></panel>
```

- rejects: show by default, hide when token exists

```
<panel rejects="$myPanel$"></panel>
```

# depends Attribute – Example

depends Attribute - Example

Event Count by Sourcetype

sourcetype =	count
access_combined	32053
cisco_esa	3819
cisco_firewall	126
cisco_wsa_squid	2478
history_access	2398
linux_secure	13018
sales_entries	56192
sendmail_syslog	1633
vendor_sales	1955
winauthentication_security	2397

depends Attribute - Example

Event Count by Sourcetype

sourcetype =	count
access_combined	32053
cisco_esa	3819
cisco_firewall	126
cisco_wsa_squid	2478
history_access	2398
linux_secure	13018
sales_entries	56192
sendmail_syslog	1633
vendor_sales	1955
winauthentication_security	2397

Recent events for access\_combined

Time	Sourcetype	Count
2019-02-26 10:20:42	access_combined	32053
2019-02-26 10:20:42	access_combined	3819
2019-02-26 10:20:42	access_combined	126
2019-02-26 10:20:42	access_combined	2478
2019-02-26 10:20:42	access_combined	2398
2019-02-26 10:20:42	access_combined	13018
2019-02-26 10:20:42	access_combined	56192
2019-02-26 10:20:42	access_combined	1633
2019-02-26 10:20:42	access_combined	1955
2019-02-26 10:20:42	access_combined	2397

Click anywhere to capture the value of the sourcetype field and pass it to panel on the right.

1

2

depends Attribute - Example

Event Count by Sourcetype

sourcetype =	count
access_combined	32124
cisco_esa	3869
cisco_firewall	126
cisco_wsa_squid	2497
history_access	2401
linux_secure	13125
sales_entries	56297
sendmail_syslog	1641
vendor_sales	1957
winauthentication_security	2402

Recent events for \$selected\_value\$

Time	Sourcetype	Count
2019-02-26 10:20:42	access_combined	32124
2019-02-26 10:20:42	access_combined	3869
2019-02-26 10:20:42	access_combined	126
2019-02-26 10:20:42	access_combined	2497
2019-02-26 10:20:42	access_combined	2401
2019-02-26 10:20:42	access_combined	13125
2019-02-26 10:20:42	access_combined	56297
2019-02-26 10:20:42	access_combined	1641
2019-02-26 10:20:42	access_combined	1957
2019-02-26 10:20:42	access_combined	2402

depends Attribute - Example

Event Count by Sourcetype

sourcetype =	count
access_combined	32124
cisco_esa	3869
cisco_firewall	126
cisco_wsa_squid	2497
history_access	2401
linux_secure	13125
sales_entries	56297
sendmail_syslog	1641
vendor_sales	1957
winauthentication_security	2402

Recent events for \$selected\_value\$

Time	Sourcetype	Count
2019-02-26 10:20:42	access_combined	32124
2019-02-26 10:20:42	access_combined	3869
2019-02-26 10:20:42	access_combined	126
2019-02-26 10:20:42	access_combined	2497
2019-02-26 10:20:42	access_combined	2401
2019-02-26 10:20:42	access_combined	13125
2019-02-26 10:20:42	access_combined	56297
2019-02-26 10:20:42	access_combined	1641
2019-02-26 10:20:42	access_combined	1957
2019-02-26 10:20:42	access_combined	2402

depends Attribute - Example

Event Count by Sourcetype

sourcetype =	count
access_combined	32124
cisco_esa	3869
cisco_firewall	126
cisco_wsa_squid	2497
history_access	2401
linux_secure	13125
sales_entries	56297
sendmail_syslog	1641
vendor_sales	1957
winauthentication_security	2402

Recent events for \$selected\_value\$

Time	Sourcetype	Count
2019-02-26 10:20:42	access_combined	32124
2019-02-26 10:20:42	access_combined	3869
2019-02-26 10:20:42	access_combined	126
2019-02-26 10:20:42	access_combined	2497
2019-02-26 10:20:42	access_combined	2401
2019-02-26 10:20:42	access_combined	13125
2019-02-26 10:20:42	access_combined	56297
2019-02-26 10:20:42	access_combined	1641
2019-02-26 10:20:42	access_combined	1957
2019-02-26 10:20:42	access_combined	2402

```

<dashboard>
  <label>depends Attribute - Example</label>
  <row>
    <panel>
      <title>Event Count by Sourcetype</title>
      <table>
        <search>
          <query>index=main | stats count by sourcetype</query>
          <earliest>-7d@d</earliest>
          <latest>now</latest>
          <sampleRatio>1</sampleRatio>
        </search>
        <option name="count">20</option>
        <drilldown>
          <set token="myPanel">true</set>
          <set token="selected_value">$click.value$</set>
        </drilldown>
      </table>
    </panel>
    <panel depends="$myPanel$">
      <title>Recent events for $selected_value$</title>
      <event>
        <search>
          <query>index=main sourcetype=$selected_value$</query>
          <earliest>-7d@d</earliest>
          <latest>now</latest>
          <sampleRatio>1</sampleRatio>
        </search>
        <option name="count">5</option>
        <drilldown>
          <unset token="myPanel"></unset>
          <unset token="selected_value"></unset>
        </drilldown>
      </event>
    </panel>
  </row>
</dashboard>
  
```

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Form Input Event Handler

- <change>
- Set and unset tokens based on user input selections
- Access an input label or choice using predefined tokens
  - **label**: captures label of an input
  - **value**: captures value of an input choice
- Available for these inputs:
  - Checkbox, dropdown, link, radio, text, time

```
<input type="radio">
<change>
<set token="MyInputName">$label$</set>
<set token="MyInputChoice">$value$</set>
</change>
</input>
```

Example

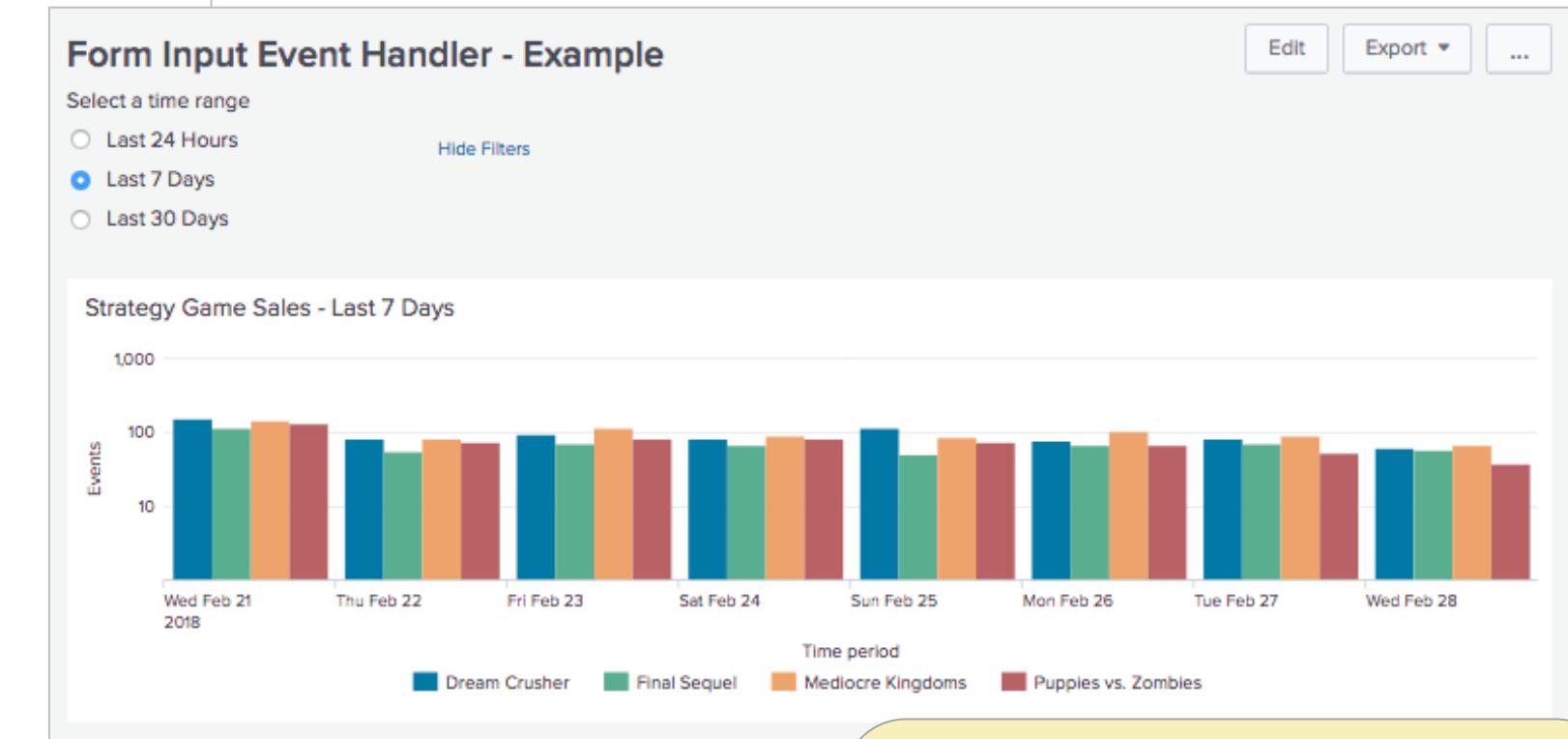
- Handler: <change>
- Input: radio button
- Event Action: set token

## Syntax

```
<change>
<eval> | <link> | <set> | <unset>
```

# Form Input Event Handler – Example 1

```
<form>
<label>Form Input Event Handler - Example</label>
<fieldset submitButton="false">
<input type="radio">
  <label>Select a time range</label>
  <choice value="-24h@h">Last 24 Hours</choice>
  <choice value="-7d@d">Last 7 Days</choice>
  <choice value="-30d@d">Last 30 Days</choice>
  <default>Last 24 Hours</default>
<change>
  <set token="date_label_tok">$label$</set>
  <set token="earliest_tok">$value$</set>
</change>
</input>
</fieldset>
<row>
<panel>
  <title>Strategy Game Sales - $date_label Tok$</title>
  <chart>
    <search>
      <query>index=main sourcetype="access_combined" categoryId=STRATEGY
        | timechart count by product_name usenull=f</query>
      <earliest>$earliest_tok$</earliest>
      <latest>now</latest>
    </search>
    ...
  </panel>
</row>
```



Example: Use a form input's label and value in a panel title and search

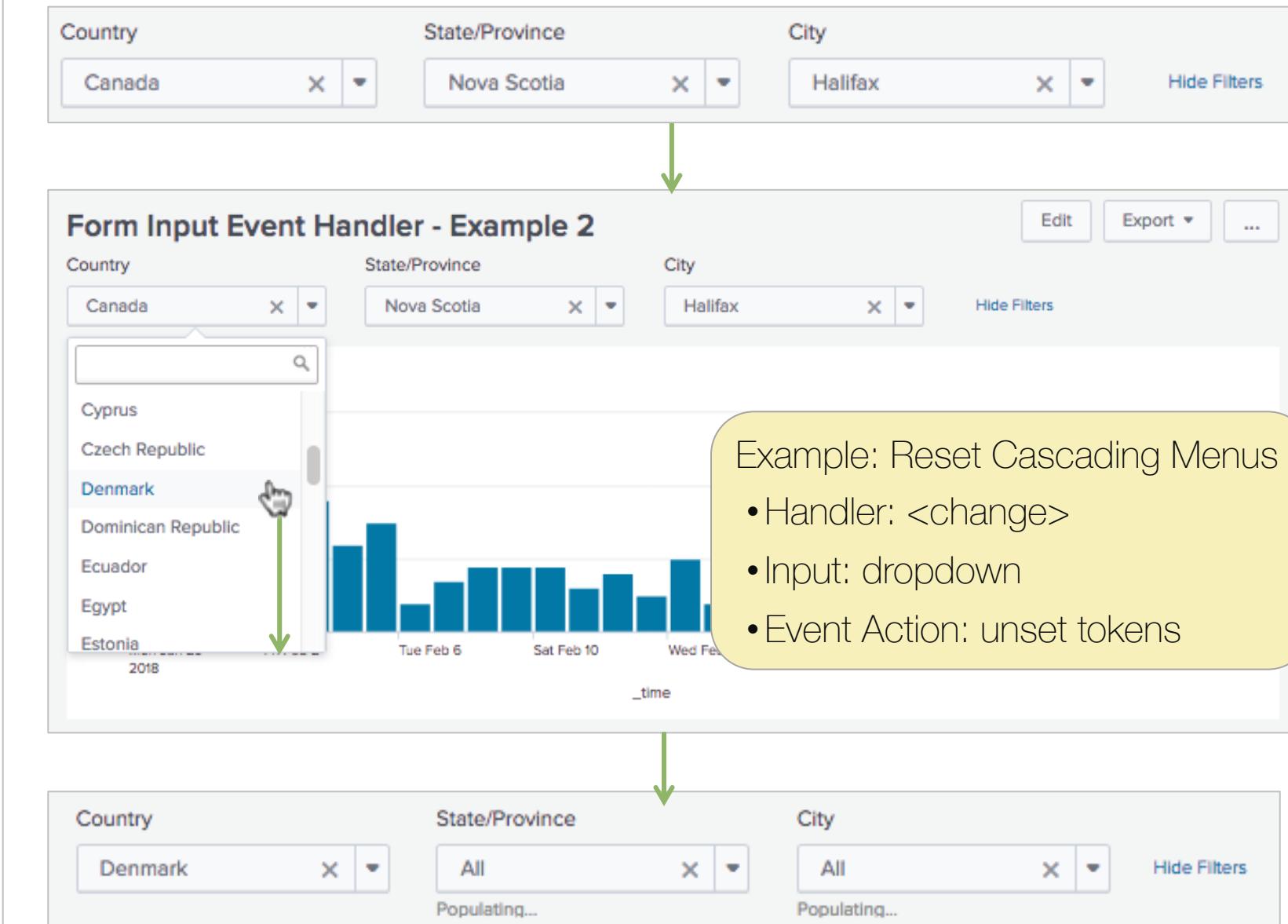
- Handler: <change>
- Input: radio button
- Event Action: set token

# Form Input Event Handler – Example 2

```
...
<fieldset submitButton="false">
<input type="dropdown" token="v_country_tok" searchWhenChanged="true">
<label>Country</label>
<choice value="*">All</choice>
<default>*</default>
<fieldForLabel>VendorCountry</fieldForLabel>
<fieldForValue>VendorCountry</fieldForValue>
<search>
<query>| inputlookup bcg_vendors | stats count by "VendorCountry"</query>
<earliest>-7d@h</earliest>
<latest>now</latest>
</search>
<change>
<unset token="form.v_state_tok"></unset>
<unset token="form.v_city_tok"></unset>
</change>
</input>

<input type="dropdown" token="v_state_tok" searchWhenChanged="true">
<label>State/Province</label>
<choice value="*">All</choice>
<default>*</default>
<fieldForLabel>VendorStateProvince</fieldForLabel>
<fieldForValue>VendorStateProvince</fieldForValue>
<search>
<query>| inputlookup bcg_vendors | search VendorCountry=$v_country Tok | stats count by "VendorStateProvince"</query>
<earliest>-7d@h</earliest>
<latest>now</latest>
</search>
<change>
<unset token="form.v_city_tok"></unset>
</change>
</input>
...

```



Example: Reset Cascading Menus

- Handler: <change>
- Input: dropdown
- Event Action: unset tokens

# Search Event Handler

- <progress>, <done>, <cancelled>, <error>, <fail>
- Access search results or search job properties using predefined tokens
- Predefined tokens:
  - **result.<field>**  
captures named value from the first row of returned results
  - **job.<property>**  
captures named job property's value

```
<search>
  <query>index=main sourcetype="access_combined"
    | timechart count by product_name usenull=f
  </query>
  <earliest>-7d@d<earliest>
  <latest>now</latest>
  <done>
    <set token="MyEventCount">$job.eventCount$</set>
  </done>
</search>
```

Example: Capture the number of events returned by a search

- Handler: <done>
- Job Property: eventCount
- Event Action: set token

## Syntax

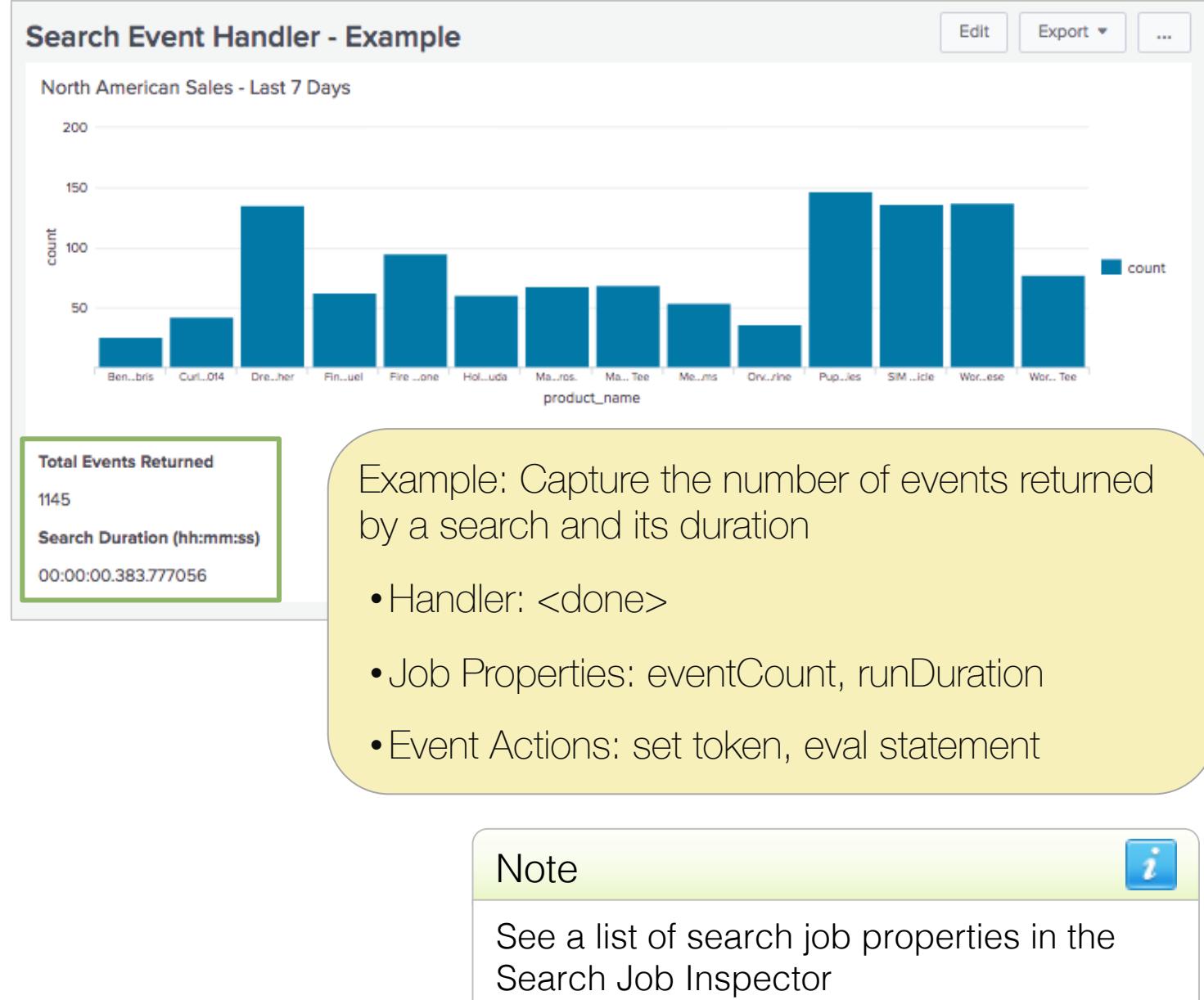
```
<search>
  <progress> | <done> | <cancelled> | <error> | <fail>
  (<eval> | <link> | <set> | <unset> | <condition>)
```

# Search Event Handler – Example

```
<dashboard>
<label>Search Event Handler - Example</label>
<row>
  <panel>
    <title>North American Sales - Last 7 Days</title>
    <chart>
      <search>
        <done>
          <eval token="mySearchDuration">tostring(tonumber('job.runDuration'),"duration")</eval>
          <set token="myEventCount">$job.eventCount$</set>
        </done>

        <query>sourcetype=vendor_sales VendorID<4000 | chart count by product_name</query>
        <earliest>-7d@h</earliest>
        <latest>now</latest>
        <sampleRatio>1</sampleRatio>
      </search>
      <option name="charting.chart">column</option>
      <option name="refresh.display">progressbar</option>
    </chart>

    <html>
      <h3>Total Events Returned</h3>
      <div>$myEventCount$</div>
      <br/>
      <h3>Search Duration (hh:mm:ss)</h3>
      <div>$mySearchDuration$</div>
    </html>
  </panel>
</row>
</dashboard>
```



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Visualization Event Handler

- <selection>
  - Pan & Zoom
- Predefined tokens
  - start / end
    - Captures the value of the x-axis (time) at the beginning and end of a selection
    - start.<field>/end.<field>
      - Captures specified series' value in the y-axis at the beginning and end of a selection
      - selection\_earliest/selection\_latest
        - Accesses the selected time range
  - Available for: area, column, line charts

Example: Pan & Zoom  
• Handler: <selection>  
• Event Action: set token

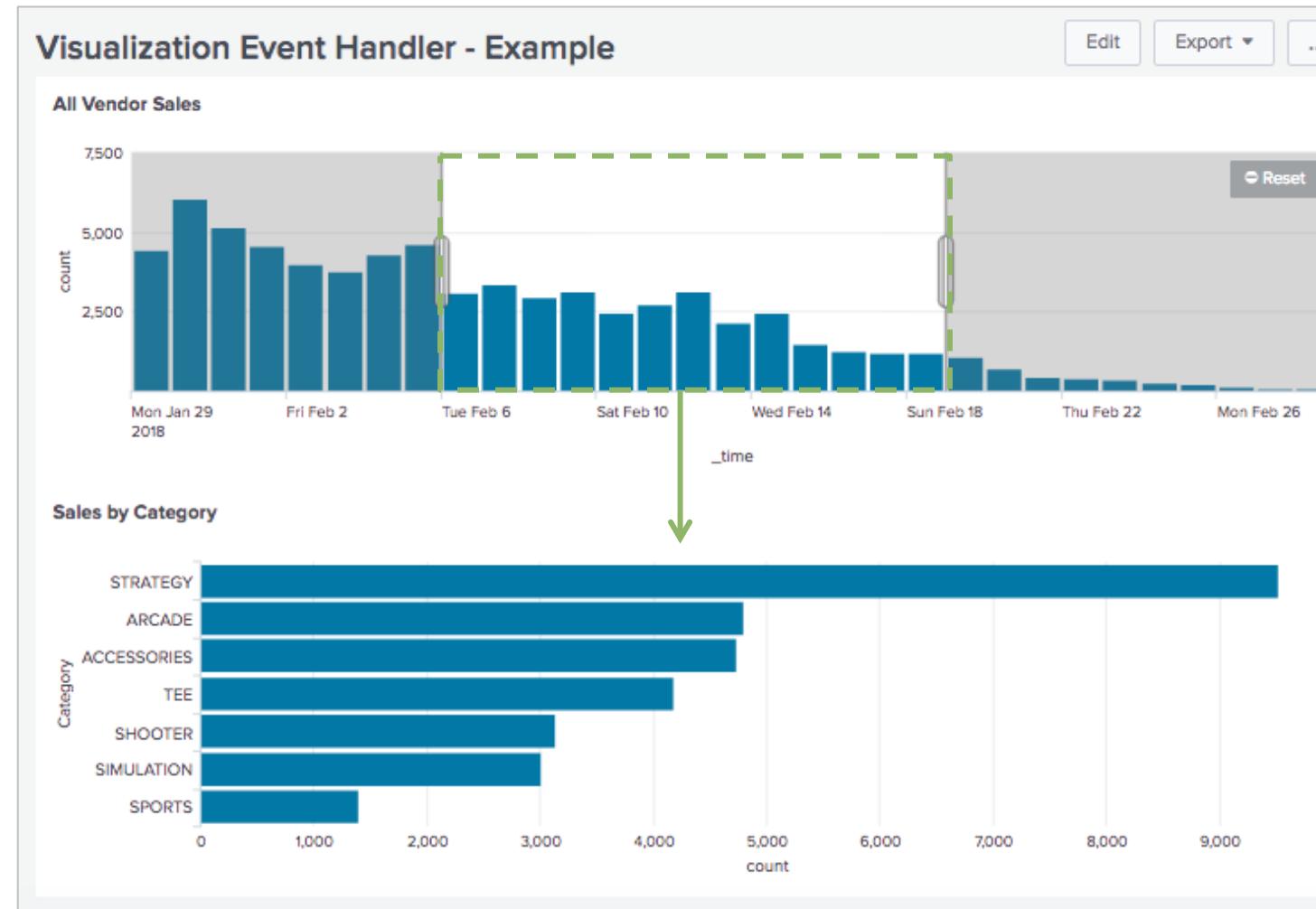
```
<chart>
...
<option name="charting.chart">column</option>
<selection>
  <set token="selection.earliest">$start$</set>
  <set token="selection.latest">$end$</set>
</selection>
</chart>
<chart>
  <title>Sales by Category</title>
  <search><query>sourcetype="vendor_sales"
    | top categoryId</query>
    <earliest>$selection.earliest$</earliest>
    <latest>$selection.latest$</latest>
  </search>
  <option name="charting.chart">bar</option>
</chart>
...
```

## Syntax

```
<[visualization]>
  <selection>
    (<eval> | <link> | <set> | <unset> )
```

# Visualization Event Handler – Example

Predefined tokens implement the selection on a chart



Example: Pan & Zoom

- Handler: <selection>
- Event Action: set token

```
<dashboard>
  <label>Selection Event Handler</label>
  <row>
    <panel>
      <chart>
        <title>All Vendor Sales</title>
        <search>
          <query>sourcetype=vendor_sales | timechart count</query>
          <earliest>0</earliest>
          <latest></latest>
        </search>
        <selection>
          <set token="selection.earliest">$start$</set>
          <set token="selection.latest">$end$</set>
        </selection>
      </chart>
      <chart>
        <title>Sales by Category</title>
        <search>
          <query>sourcetype="vendor_sales" | top categoryId
          | rename categoryId as Category</query>
          <earliest>$selection.earliest$</earliest>
          <latest>$selection.latest$</latest>
        </search>
        ...
      </chart>
    </panel>
  </row>

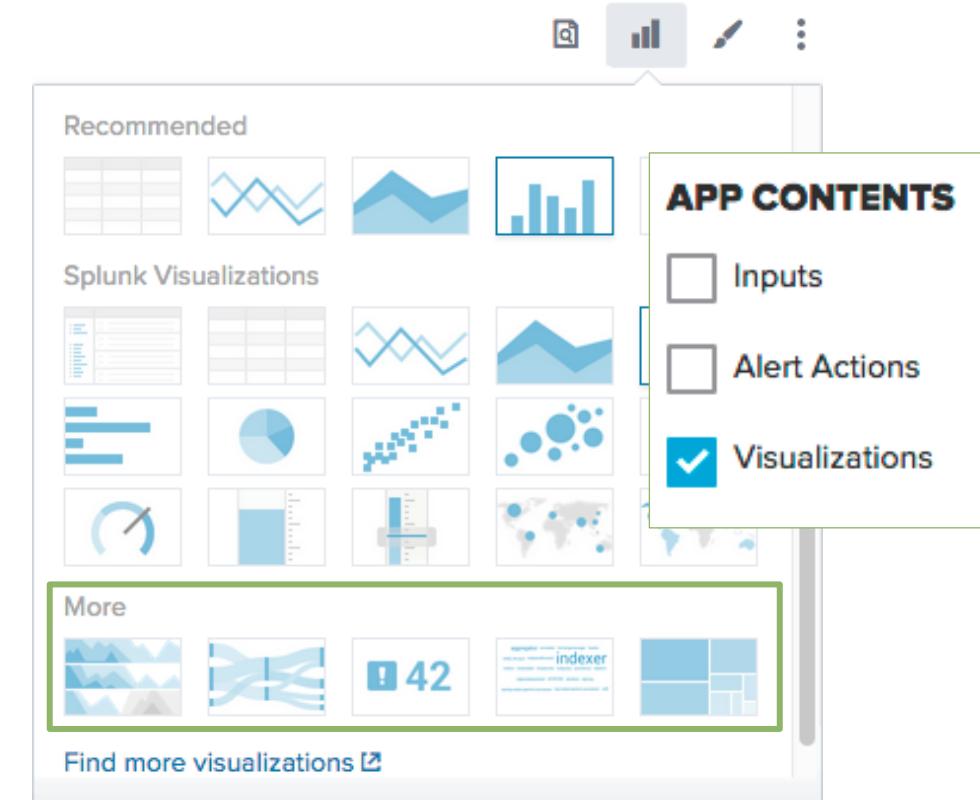
```

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Custom Visualizations



- Shareable visualizations
- Distributed with an app
- Install from splunkbase or build your own
- Many Splunk supported including:
  - Horizon Chart
  - Horseshoe Meter
  - Punchcard
  - Status Indicator
  - Treemap
  - Location Tracker
  - Parallel Coordinates
  - Timeline
  - Bullet Graph
  - Sankey Chart
  - Calendar Heat Map

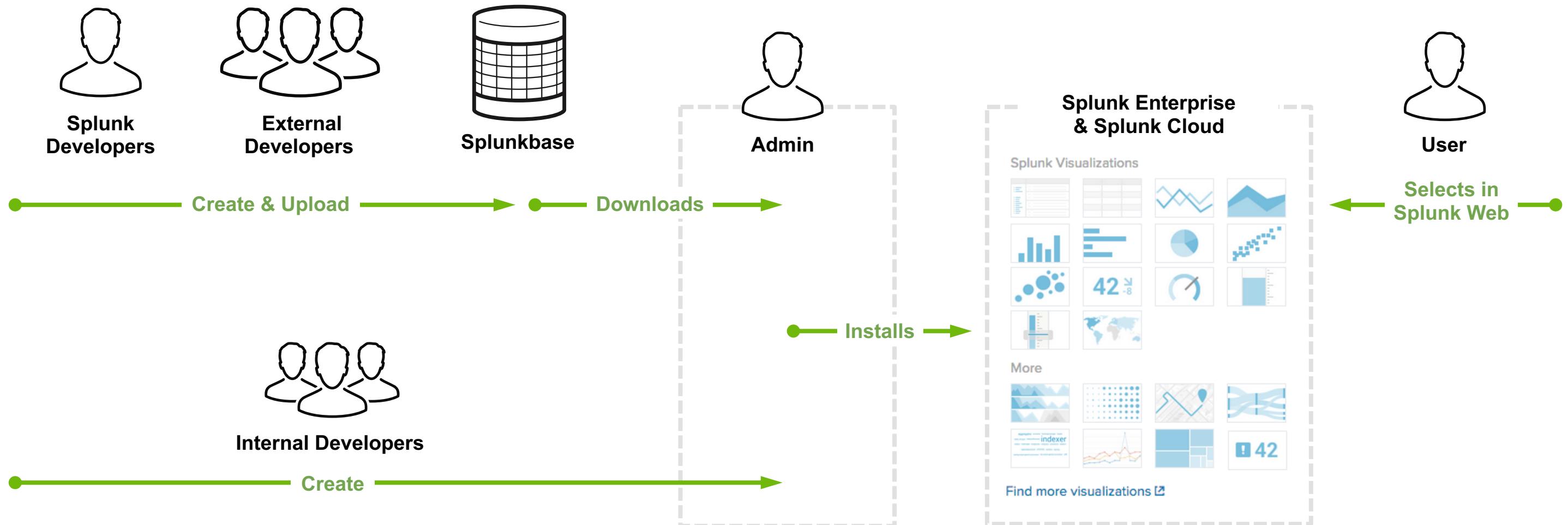


Note



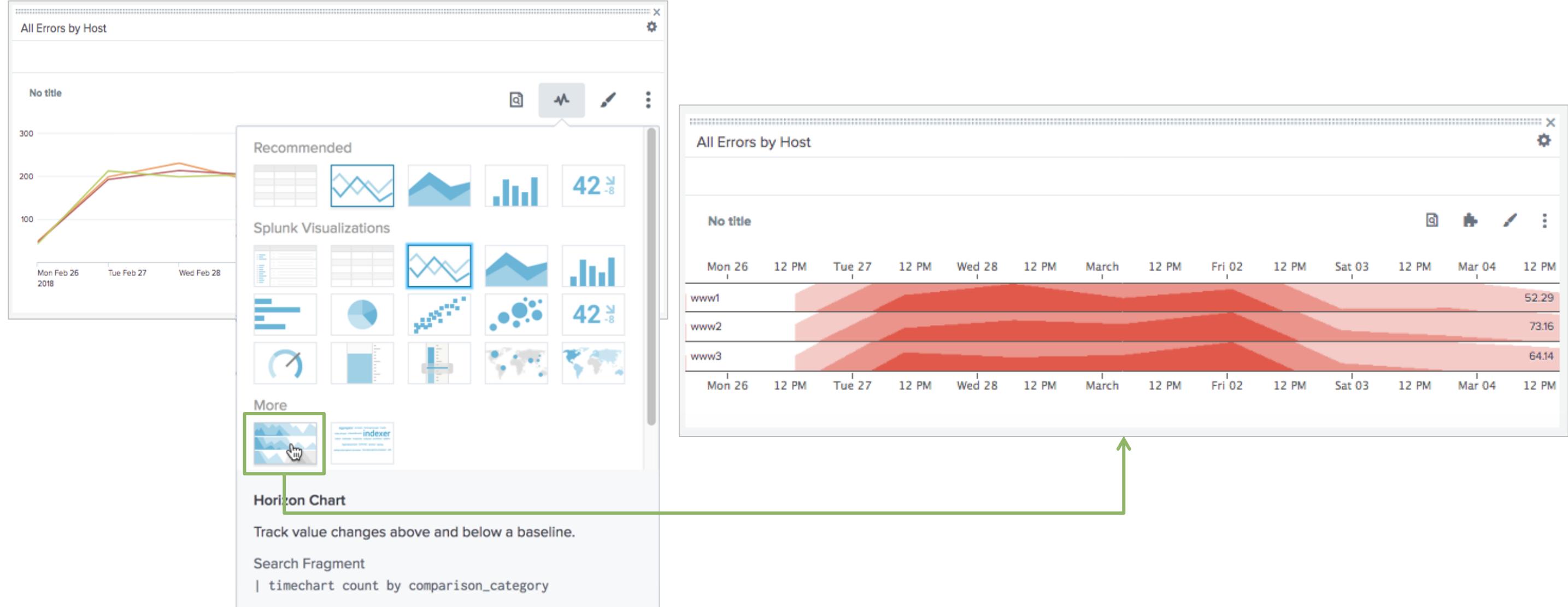
Custom Visualizations are shareable on splunkbase. See: [splunkbase.com](https://splunkbase.com)

# Custom Visualizations (cont.)



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Custom Visualizations – Example

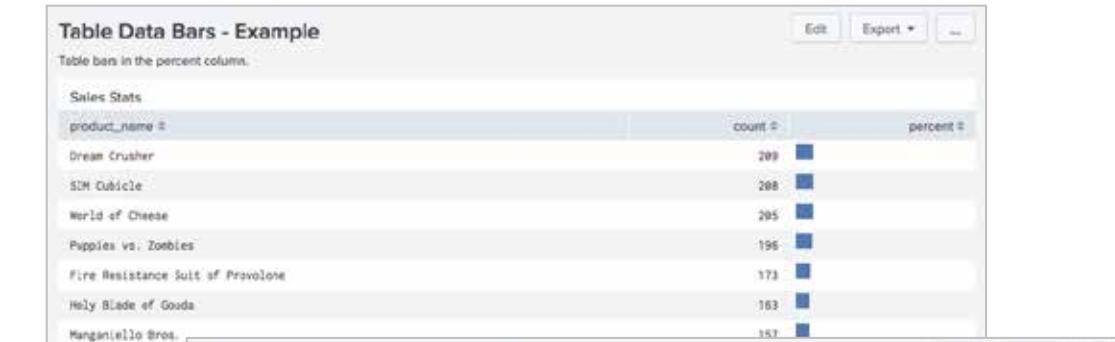


Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Simple XML Extensions



- Customize a view's look and behavior with your custom CSS and JavaScript
- Examples:
  - Stylesheet: use a custom CSS to make simple layout changes
  - Tables with custom renderers: use custom styles and behaviors within tables



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Simple XML Extensions (cont.)

---

- Add CSS & JS files to: `$APP_HOME/appserver/static`

- Reference them in the view's XML:

```
<dashboard script="my_script.js" stylesheet="my_style.css">
```

- Reference multiple files in the view's XML:

```
<dashboard script="my_script.js, my_script2.js"  
stylesheet="my_style.css, my_style2.css">
```

- Reference another app's files in the view's XML:

```
<dashboard script="otherApp:myVizDirectory/my_script.js"  
stylesheet="otherApp:myVizDirectory/my_style.css">
```

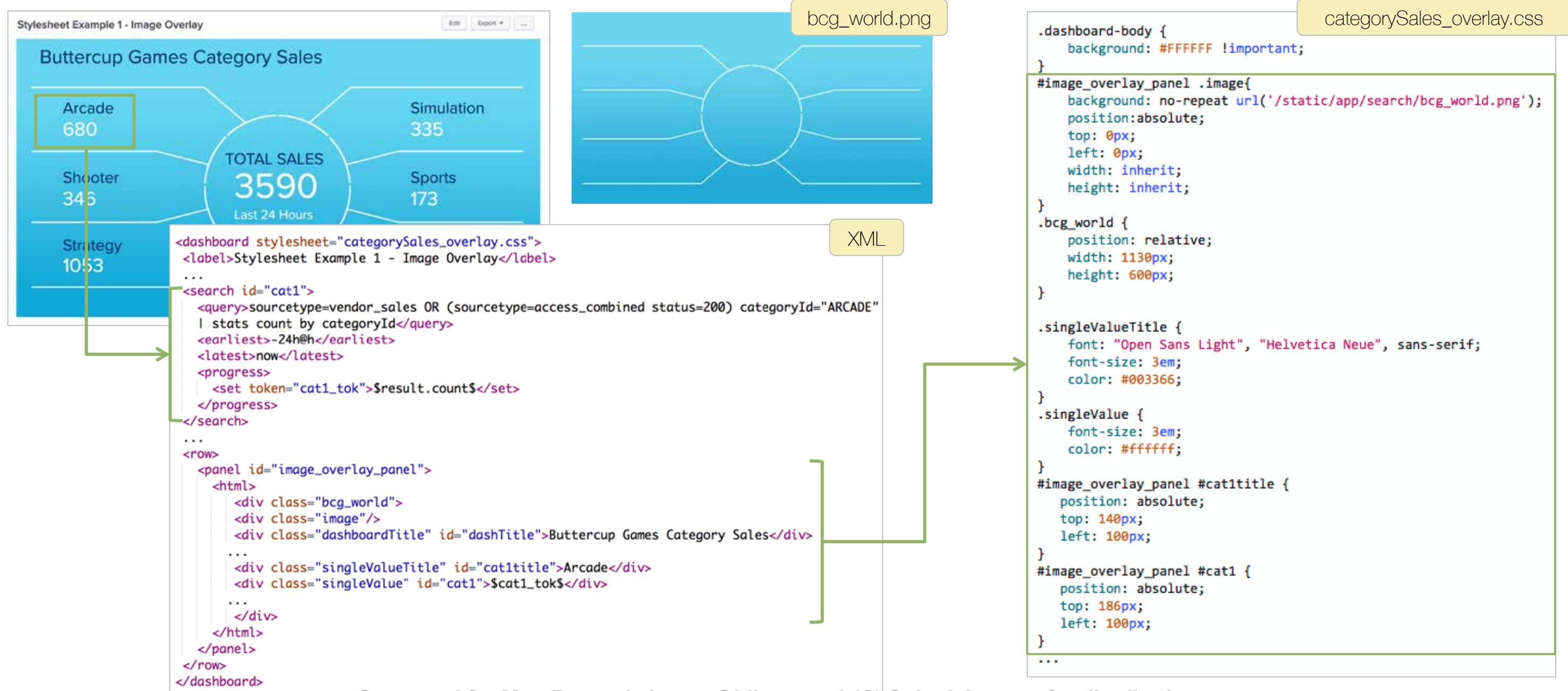
- Individual dashboards and forms:

- Upload the file(s) and reference them in the XML

- All dashboards and forms in an app

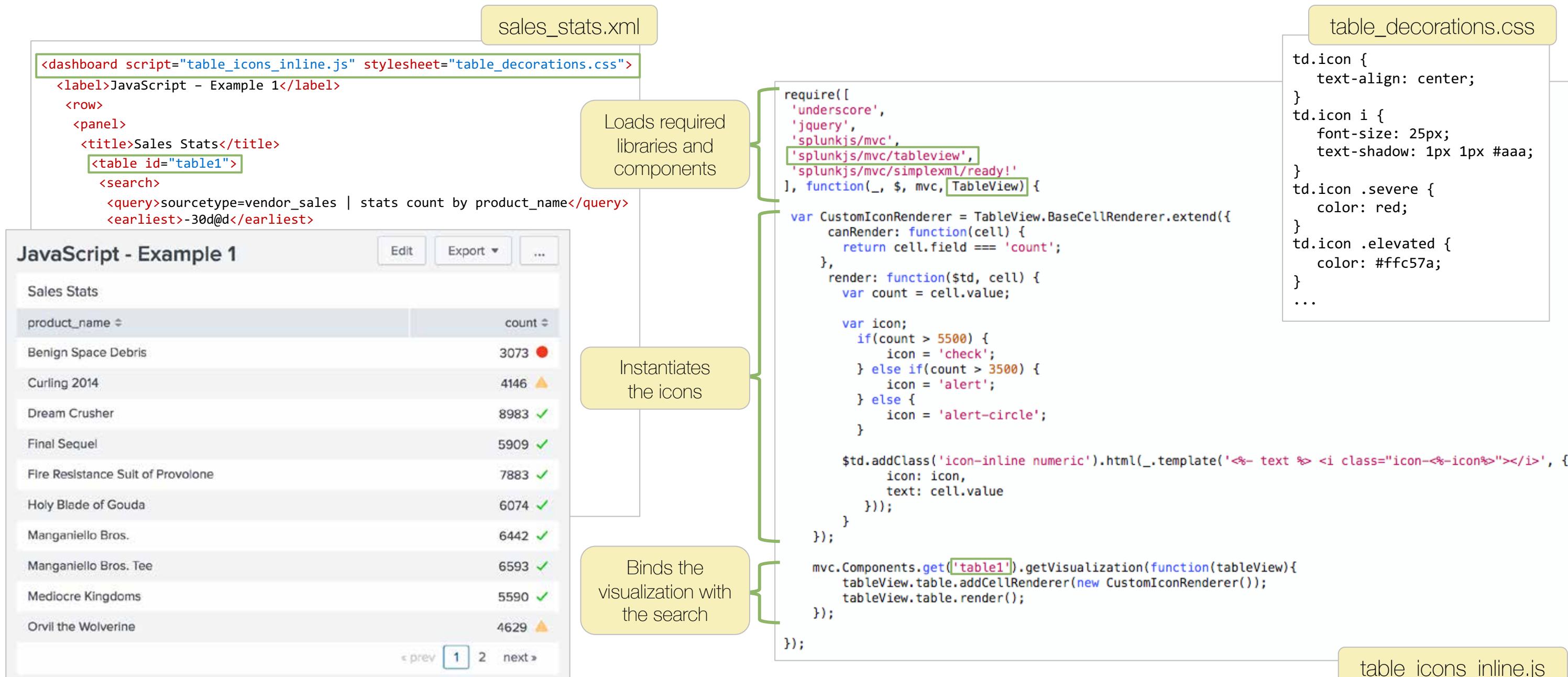
- Upload `dashboard.css` or `dashboard.js` (no XML reference)

# Stylesheet Example – Image Overlay



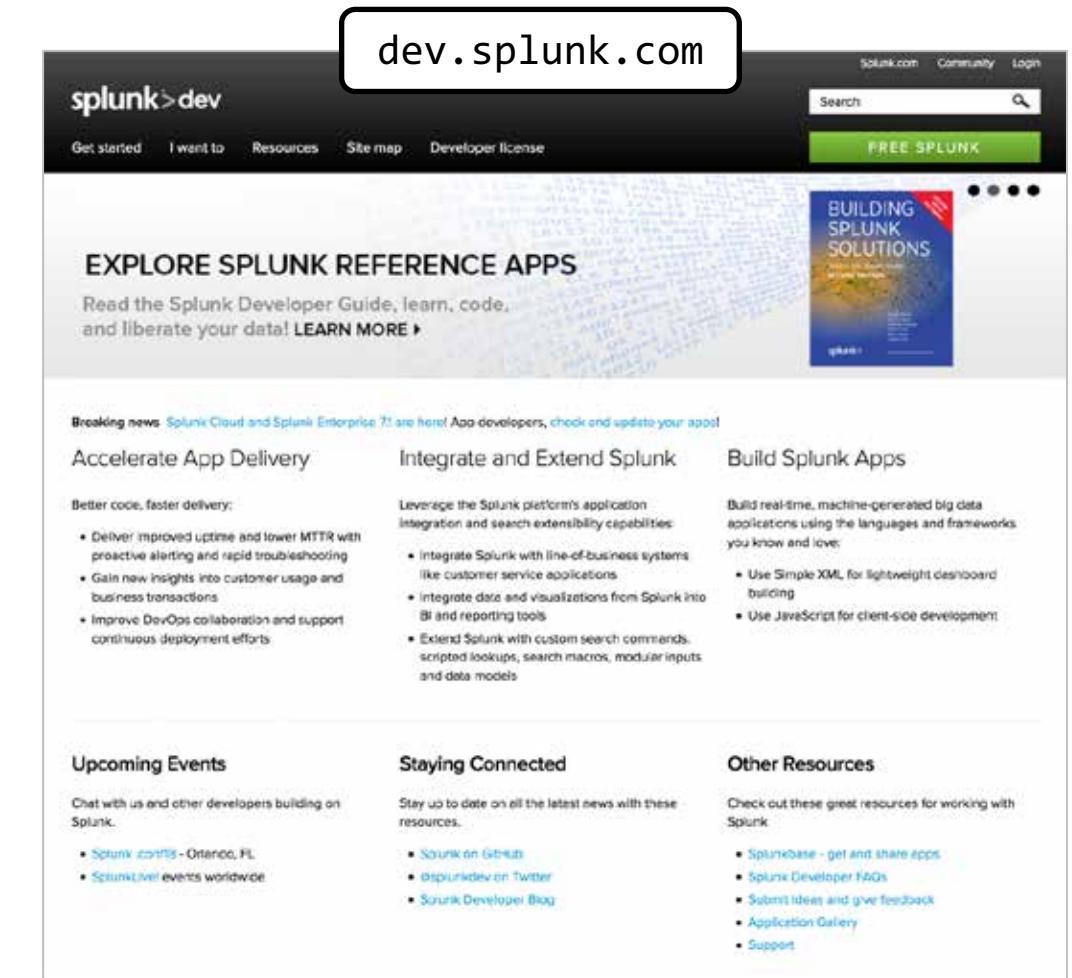
Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# JavaScript Example – Table Icons



# Useful References

- Using the Splunk Web Framework  
[dev.splunk.com/view/SP-CAAAEXG](https://dev.splunk.com/view/SP-CAAAEXG)
- Modify dashboards using Simple XML Extensions  
[dev.splunk.com/view/SP-CAAAE4A](https://dev.splunk.com/view/SP-CAAAE4A)
- Splunk platform custom visualizations API  
[dev.splunk.com/view/SP-CAAAE8Q](https://dev.splunk.com/view/SP-CAAAE8Q)



The screenshot shows the homepage of dev.splunk.com. At the top right, there is a search bar and a "FREE SPLUNK" button. Below the header, there's a banner for "BUILDING SPLUNK SOLUTIONS". The main content area includes sections for "EXPLORE SPLUNK REFERENCE APPS", "Accelerate App Delivery", "Integrate and Extend Splunk", "Build Splunk Apps", "Upcoming Events", "Staying Connected", and "Other Resources". Each section contains descriptive text and a list of bullet points.

**dev.splunk.com**

splunk>dev

Get started I want to Resources Site map Developer license

Search

FREE SPLUNK

BUILDING SPLUNK SOLUTIONS

EXPLORE SPLUNK REFERENCE APPS

Read the Splunk Developer Guide, learn, code, and liberate your data! [LEARN MORE](#)

Breaking news: Splunk Cloud and Splunk Enterprise 7.1 are here! App developers, check and update your apps!

**Accelerate App Delivery**

Better code, faster delivery:

- Deliver improved uptime and lower MTTR with proactive alerting and rapid troubleshooting
- Gain new insights into customer usage and business transactions
- Improve DevOps collaboration and support continuous deployment efforts

**Integrate and Extend Splunk**

Leverage the Splunk platform's application integration and search extensibility capabilities:

- Integrate Splunk with line-of-business systems like customer service applications
- Integrate data and visualizations from Splunk into BI and reporting tools
- Extend Splunk with custom search commands, scripted lookups, search macros, modular inputs, and data models

**Build Splunk Apps**

Build real-time, machine-generated big data applications using the languages and frameworks you know and love:

- Use Simple XML for lightweight dashboard building
- Use JavaScript for client-side development

**Upcoming Events**

Chat with us and other developers building on Splunk.

- [Splunk conf18 - Orlando, FL](#)
- [SplunkDev events worldwide](#)

**Staying Connected**

Stay up to date on all the latest news with these resources.

- [Splunk on GitHub](#)
- [SplunkDev on Twitter](#)
- [Splunk Developer Blog](#)

**Other Resources**

Check out these great resources for working with Splunk.

- [Splunkbase - get and share apps](#)
- [Splunk Developer FAQs](#)
- [Submit Ideas and give Feedback](#)
- [Application Gallery](#)
- [Support](#)

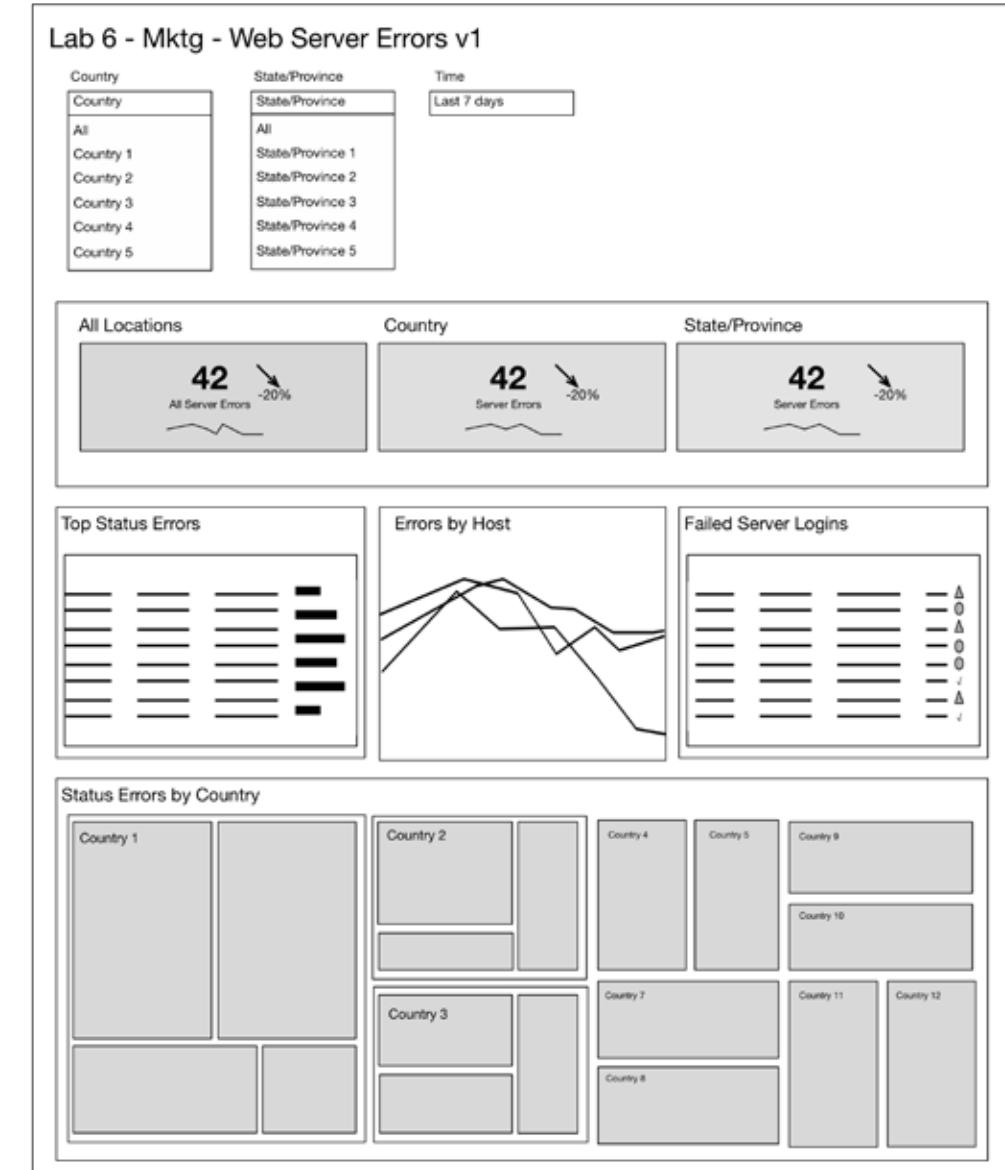
# Lab 6 – Add Advanced Behavior & Visualizations

Time: 40 minutes

Scenario: The marketing team would like a form that displays metrics for web store server errors, status errors, and failed server logins.

Tasks:

- Create a dashboard
- Add two cascading inputs and a time input
- Add custom multiselect input behavior
- Add three prebuilt panels and convert to inline
- Add a chart and two table panels
- Display a data bar in a table cell
- Configure a dynamic display panel
- Display icons in a table cell
- Add a Splunk Custom Visualization



# Summary

Generated for Matt Brown ([mbrown@idbny.com](mailto:mbrown@idbny.com)) (C) Splunk Inc, not for distribution

# Wrap-up

---

- You should now be able to:
  - Apply best practices when creating views
  - Capture and access dynamic values
  - Optimize dashboard performance
  - Create well formed, global searches
  - Customize dashboard appearance
  - Create dynamic drilldowns and behaviors
  - Troubleshoot views

# Next Steps

## Apps & Add-ons

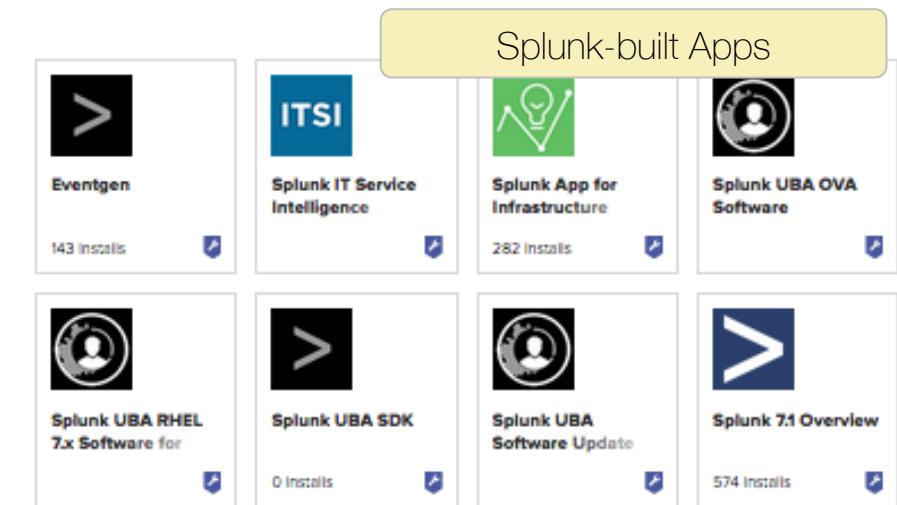
- Splunk Dashboard Examples
- Custom Visualizations

## Courses

- Fundamentals 3
- Advanced Dashboards & Visualizations
- Building Splunk Apps
- Developing with Splunk's REST API
- Splunk Data Administration
- Splunk System Administration

## Certification Tracks

[https://www.splunk.com/en\\_us/training.html#certificationtrack](https://www.splunk.com/en_us/training.html#certificationtrack)



# Community

---

- **Splunk Community Portal**

[splunk.com/en\\_us/community.html](http://splunk.com/en_us/community.html)

- **Splunk Answers**

[answers.splunk.com](http://answers.splunk.com)

- **Splunk Apps**

[splunkbase.com](http://splunkbase.com)

- **Splunk Blogs**

[splunk.com/blog/](http://splunk.com/blog/)

- **Splunk Live!**

[splunklive.splunk.com](http://splunklive.splunk.com)

- **.conf**

[conf.splunk.com](http://conf.splunk.com)

- **Slack User Groups**

[splk.it/slack](http://splk.it/slack)

- **Splunk Dev Google Group**

[groups.google.com/forum/#!forum/splunkdev](http://groups.google.com/forum/#!forum/splunkdev)

- **Splunk Docs on Twitter**

[twitter.com/splunkdocs](http://twitter.com/splunkdocs)

- **Splunk Dev on Twitter**

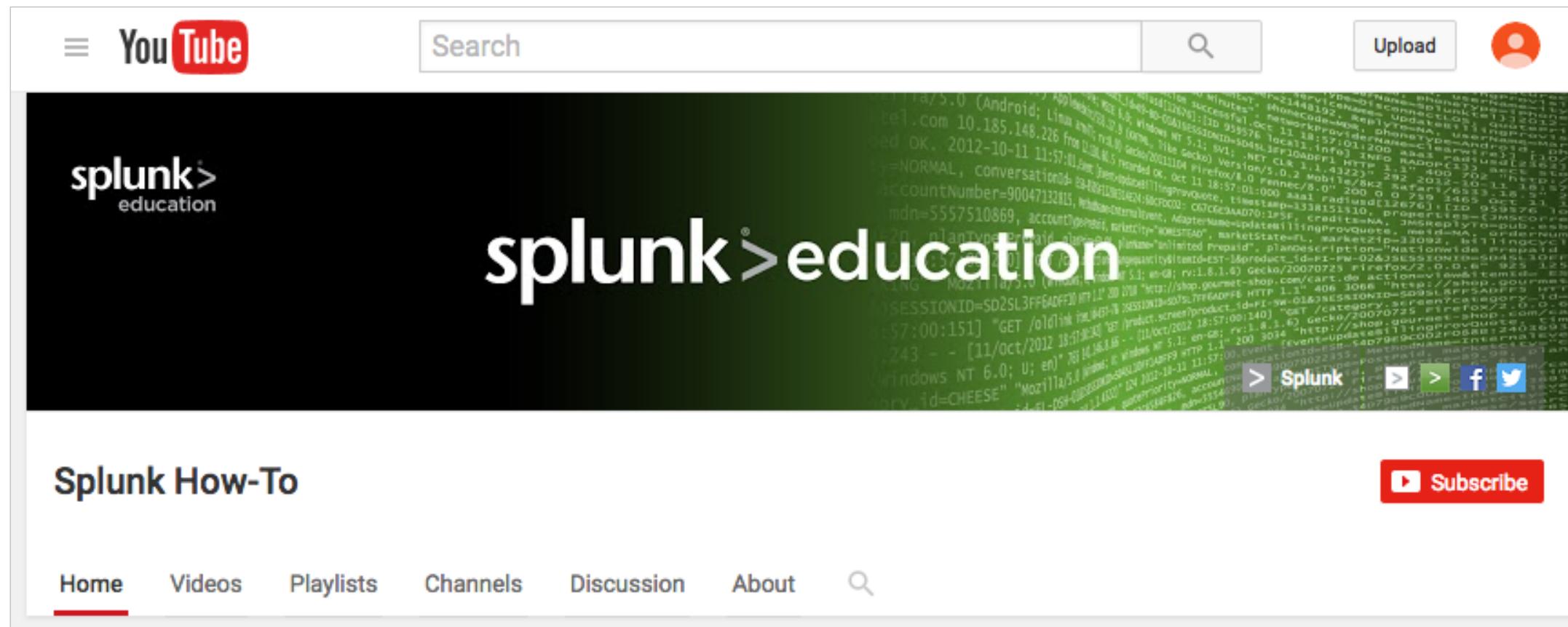
[twitter.com/splunkdev](http://twitter.com/splunkdev)

- **IRC Channel**

#splunk on the EFNet IRC server

# Splunk How-To Channel

- Check out the Splunk Education How-To channel on YouTube:  
<http://splk.it/How-To>
- Free, short videos on a variety of Splunk topics



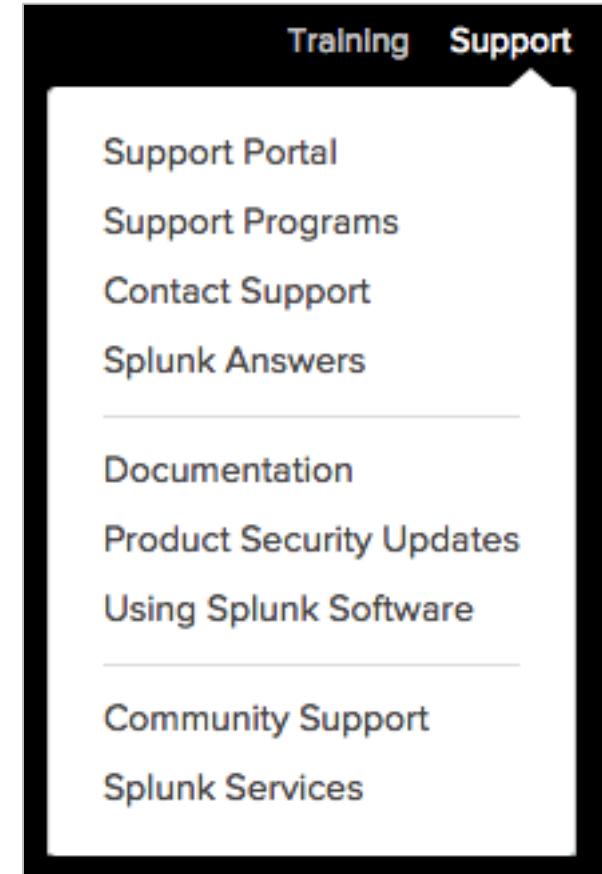
Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution

# Support Programs

- **Web**
  - Documentation: dev.splunk.com and docs.splunk.com
  - Wiki: wiki.splunk.com
- **Global Support**

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

  - Web: splunk.com/index.php/submit\_issue
  - Phone: (855) SPLUNK-S or (855) 775-8657
- **Enterprise Support**
  - Access customer support by phone and manage your cases online 24 x 7 (depending on support contract)



Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc, not for distribution



splunk®>

.conf19

.conf19

October 21-24, 2019

Splunk University

October 19-21, 2019

Las Vegas, NV

The Venetian Sands Expo



4 Days of Innovation



350 Education Sessions



20 Hours of Networking

Generated for Matt Brown (mbrown@idbny.com) (C) Splunk Inc. not for distribution

sign up for notifications @ [conf.splunk.com](http://conf.splunk.com)



Generated for Matt Brown ([mbrown@idbny.com](mailto:mbrown@idbny.com)) (C) Splunk Inc, not for distribution