



Creating Knowledge Objects

# Document Usage Guidelines

---

- Should be used only for enrolled students
- Not meant to be a self-paced document, an instructor is needed
- Lab Exercise slides reference the hands-on lab exercise guide
- Do not distribute

# Course Goals

---

- Create search macros
- Create event types
- Understand event types and use the event type builder
- Compare event types and reports
- Create workflow actions
- Create tags and aliases
- Create calculated fields

# Course Outline

---

- Knowledge Objects and Search-time Operations
- Create Event Types
- Create Workflow Actions
- Create Tags and Aliases
- Create Search Macros
- Create Calculated Fields

# Knowledge Objects & Search-time Operations

# Topic Objectives

---

- Understand role of knowledge objects for enriching data
- Define search-time operation sequence

# Knowledge Objects

---

- Knowledge objects are user-defined entities that can be used to enrich data and retrieve specific information about data
- Can be shared or used privately
- The following knowledge objects are discussed in this course:
  - Event types
  - Workflow actions
  - Tags
  - Field aliases
  - Search macros
  - Calculated fields

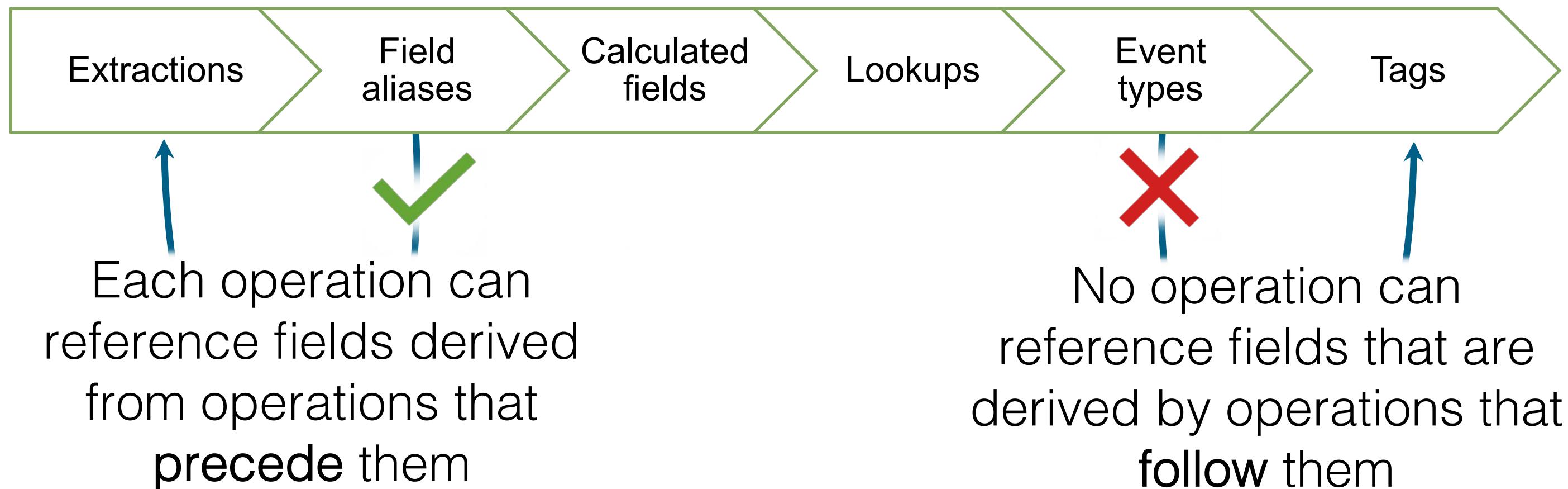
# Search-time Operation Sequence

After running a search, Splunk performs a specific sequence of operations to pull knowledge objects and apply them to the events returned by the search



# Search-time Operation Sequence

Search-time operations are always applied in the same order when generating the knowledge objects



# Create Event Types

# Topic Objectives

---

- Define event types
- Create event types using:
  - New Event Type
  - Search page
  - Event Type Builder
- Use Event Types
- Find Event Types
- Tag event types
- Compare event types and reports

# Define Event Types

- Categorizes events based on a search string
- A useful method for institutional knowledge capturing and sharing
- Can be tagged to group similar types of events
- Processed after extractions, field aliases, calculated fields, and lookup in the Search Time Operation Sequence



# Create an Event Type: New Event Type

Settings > Event types > **New Event Type**

- Choose a Destination App
- Name the event type
- The Search string is the basic search that meets your event type criteria

index=web		
i	Time	Event
>	6/9/22 8:53:20.000 PM	188.173.152.100 - - [09/Jun/2022:20:53:20] "POST /cart/success.do?JSESSIONID=SD4SL5FF10ADFF4955 HTTP/1.1" 200 1426 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-21" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 780 host = www2   source = /opt/log/www2/access.log   sourcetype = access_combined

Destination App

Name \*

Search string \*

Tag(s)

Enter a comma-separated list of tags.

Color

Priority

Highest priority shows up first in a result.

Priority controls which event type  
Color displays for an event that  
match two or more event types

**Cancel** **Save**

# Create an Event Type: Search

1. Run a search and verify that all results meet your event type criteria
2. From the Save As menu, select Event Type
3. Provide a Name for your event type (name should not contain spaces)

The screenshot illustrates the process of creating an event type in Splunk:

- New Search:** A search bar contains the query `index=* status>499`. The results show 264 events from June 8, 2022, to June 9, 2022. The "Events (264)" tab is selected. A green box highlights the search bar.
- Save As Menu:** A context menu is open under the "Save As" button. The "Event Type" option is highlighted with a green box and circled with orange number 2.
- Save As Event Type Dialog:** A modal dialog titled "Save As Event Type" is shown. It has fields for Name (set to "web\_error"), Tags (Optional), Color (yellow), and Priority (1 (Highest)). A note at the bottom states: "Determines which style wins, when an event has more than one event type." A green arrow points from the "Event Type" menu option to this dialog.

**Note:** Must be a basic search (cannot contain pipes or subsearches).

# Create an Event Type: Event Type Builder

From the event details, select **Event Actions > Build Event Type**

The screenshot shows the Splunk interface for a search titled "New Search". The search bar contains the query "index=\*" status>499. The results section shows 264 events from June 8 to June 9, 2022. The "Events (264)" tab is selected. A timeline at the bottom indicates "1 hour per column". Below the timeline, a list of events is shown, with the first event highlighted. The event details show a timestamp of "6/9/22 8:46:18" and the action "Build Event Type". A context menu is open over this event, with the option "Build Event Type" highlighted and circled with a red number "2". Another red circle with the number "1" is on the "Event Actions" button at the bottom of the menu. The "Event" field is also circled with a red number "2".

# Create an Event Type: Event Type Builder (cont.)

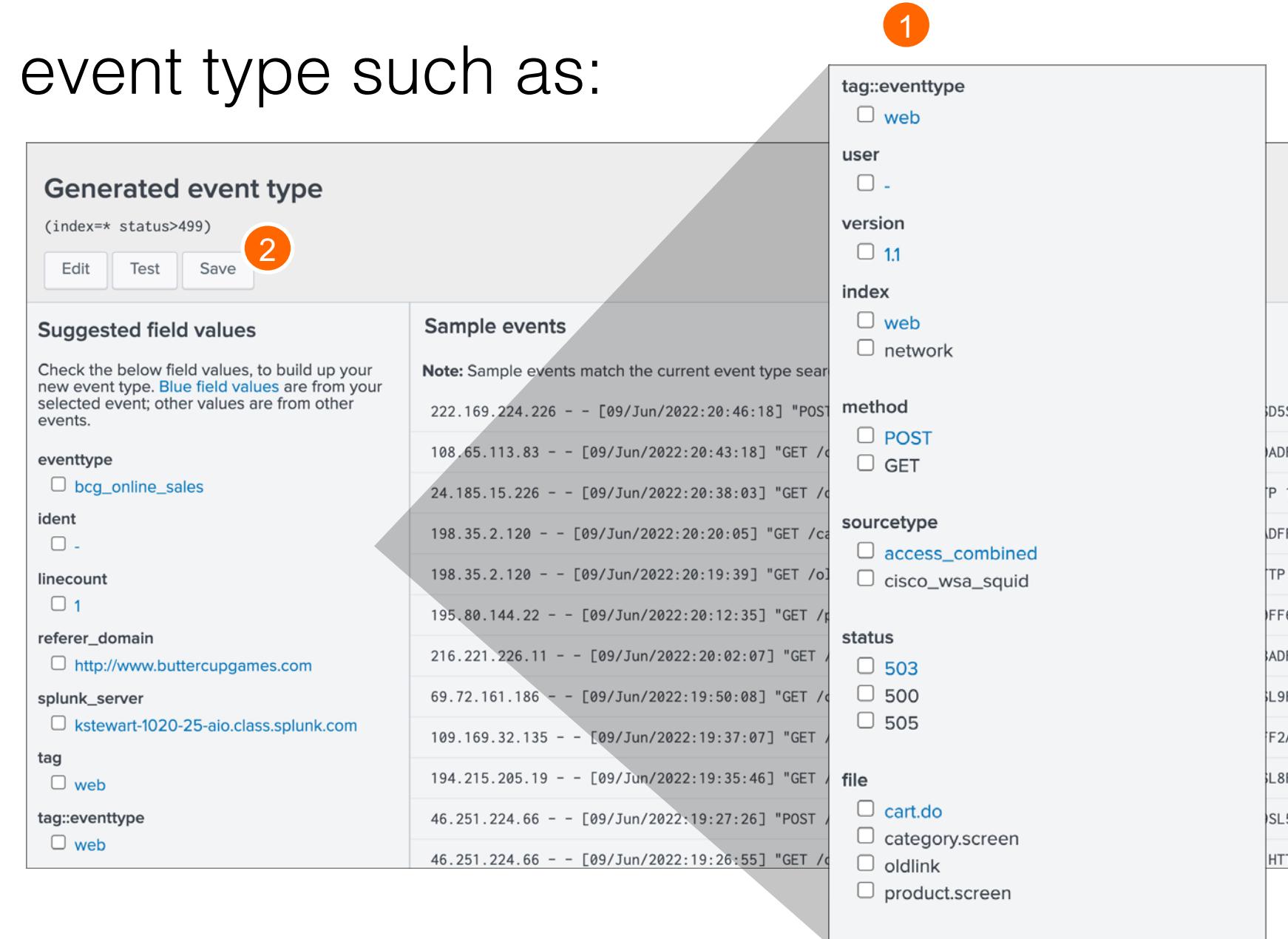
① Refine the criteria for your event type such as:

- Search string
- Field values
- Tags

② Verify your selections and click Save

**Note** 

The preferred—and easier—method for creating an event type is from the Search page, as previously shown. While the Event Type Builder can be used, it provides somewhat more limited functionality.



The screenshot shows the Splunk Event Type Builder interface. At the top, it displays a search bar with the query: `(index==* status>499)`. Below the search bar are three buttons: `Edit`, `Test`, and `Save`. A red circle with the number **2** is positioned over the `Save` button. To the right of the search bar, there is a large list of filter categories with checkboxes:

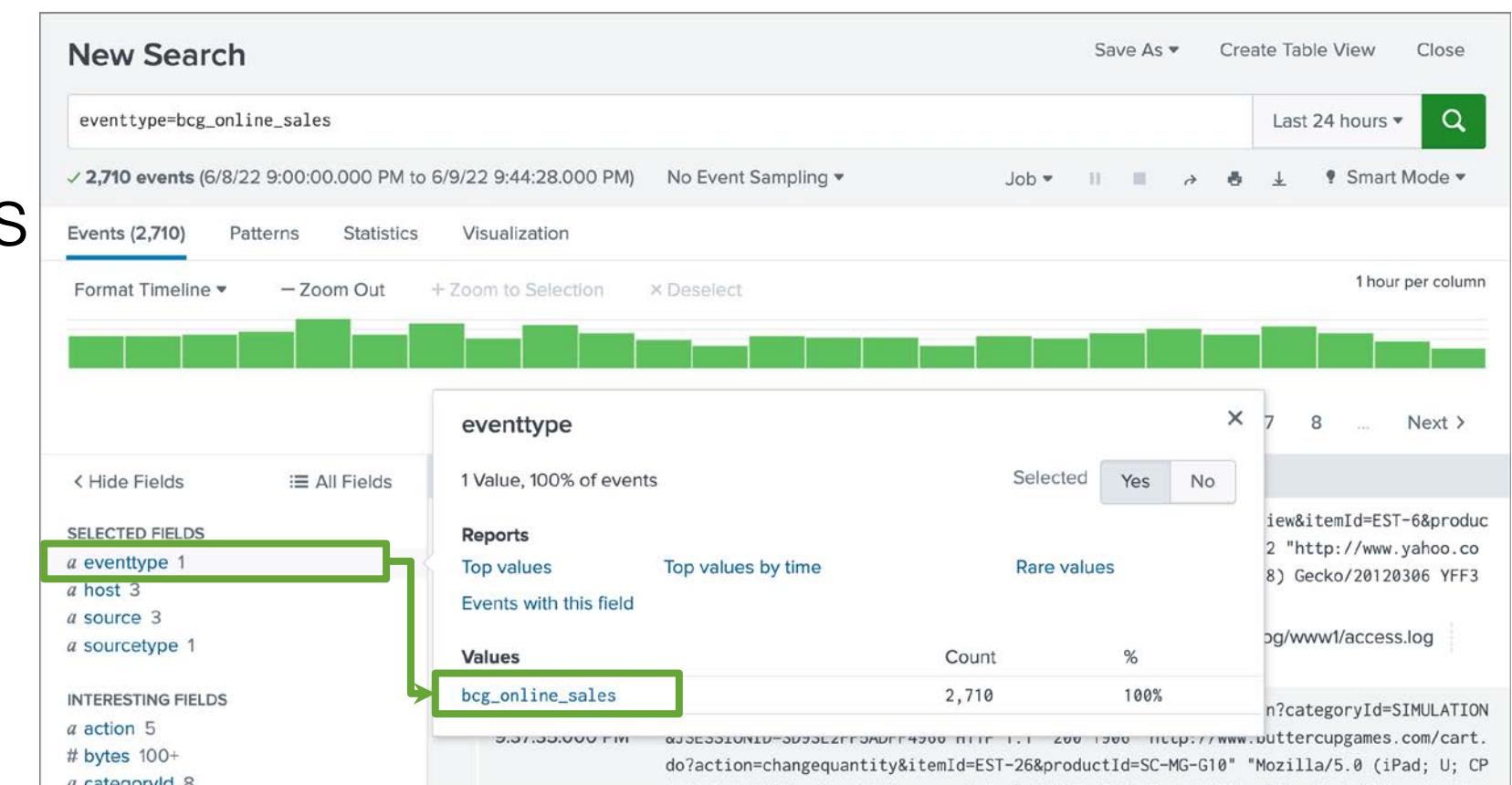
- tag:eventtype**:  `web`
- user**:  `-`
- version**:  `1.1`
- index**:  `web`  
 `network`
- method**:  `POST`  
 `GET`
- sourcetype**:  `access_combined`  
 `cisco_wsa_squid`
- status**:  `503`  
 `500`  
 `505`
- file**:  `cart.do`  
 `category.screen`  
 `oldlink`  
 `product.screen`

Below these filters, the interface is divided into two main sections:

- Suggested field values**: A list of fields and their corresponding values, many of which are highlighted in blue:
  - `eventtype`:  `bcg_online_sales`
  - `ident`:  `-`
  - `linecount`:  `1`
  - `referer_domain`:  `http://www.buttercupgames.com`
  - `splunk_server`:  `kstewart-1020-25-aio.class.splunk.com`
  - `tag`:  `web`
  - `tag:eventtype`:  `web`
- Sample events**: A list of log entries matching the current search criteria:
  - 222.169.224.226 - - [09/Jun/2022:20:46:18] "POST / HTTP/1.1"
  - 108.65.113.83 - - [09/Jun/2022:20:43:18] "GET / HTTP/1.1"
  - 24.185.15.226 - - [09/Jun/2022:20:38:03] "GET / HTTP/1.1"
  - 198.35.2.120 - - [09/Jun/2022:20:20:05] "GET /cart/do HTTP/1.1"
  - 198.35.2.120 - - [09/Jun/2022:20:19:39] "GET /oldlink HTTP/1.1"
  - 195.80.144.22 - - [09/Jun/2022:20:12:35] "GET /category.screen HTTP/1.1"
  - 216.221.226.11 - - [09/Jun/2022:20:02:07] "GET / HTTP/1.1"
  - 69.72.161.186 - - [09/Jun/2022:19:50:08] "GET / HTTP/1.1"
  - 109.169.32.135 - - [09/Jun/2022:19:37:07] "GET / HTTP/1.1"
  - 194.215.205.19 - - [09/Jun/2022:19:35:46] "GET / HTTP/1.1"
  - 46.251.224.66 - - [09/Jun/2022:19:27:26] "POST /oldlink HTTP/1.1"
  - 46.251.224.66 - - [09/Jun/2022:19:26:55] "GET /category.screen HTTP/1.1"

# Use Event Types

- To verify the event type, search for `eventtype=<event type>`
- Fields sidebar displays `eventtype`, which can be added as a selected field
- Events are evaluated and the appropriate event types are applied at search time
- Using the Fields sidebar, view event types and their statistics



# Find Created Event Types

- Settings > Event types
  - Displays event types you have permission to view or edit
  - Create new, clone, or maintain existing event types

Event types									New Event Type
Showing 1-4 of 4 items		App	Search & Reporting (s...)	Owner	Any	Visible in the App	filter	25 per page	
Name	Search string		Tag(s)	Owner	App	Sharing	Status	Actions	
bcg_online_sales	index=web sourcetype=access_combined action=""	web	admin	ao-bcg-loc	Global   Permissions	Enabled	Clone		
internal_search_terms	( "After evaluating args" OR "Before evaluating args" OR "context dispatched for search=" OR "SearchParser - PARSING" OR "got search" OR "_dispatchNewSearch - search" OR "search:* - q" OR ( decomposition fullsearch ) OR "PAAAAAARSER! - search" OR "view:* - DECOMPOSITION" OR "Splunk.Module.SearchBar .setInputField" OR ( typeahead prefix ) OR "DEBUG HTTPServer - Deleting request=GET" OR /en-US/api/search/typeahead )	No owner	system	Global   Permissions	Enabled	Clone			
splunkd-access	index=_internal source=*/splunkd_access.log OR source=*\splunkd_access.log	No owner	system	Global   Permissions	Enabled	Clone			
splunkd-log	index=_internal source=*/splunkd.log OR source=*\splunkd.log	No owner	system	Global   Permissions	Enabled	Clone			

# Tag Event Types

Event types can be tagged in two ways:

1. Settings > Event types
2. Event details > Actions

**Screenshot 1: Event types configuration**

The 'Event types' configuration page for 'web\_error'. It includes a search string 'index=\*> status>499', a 'Tag(s)' field containing 'error,web' (highlighted with a green box), a 'Color' field set to 'yellow' (highlighted with a green box), and a 'Priority' field set to '1 (Highest)' (highlighted with a green box). A note at the bottom states: 'Tags are discussed in more detail in a later topic.'

**Screenshot 2: Event Actions configuration**

The 'Event Actions' configuration page. It shows a table with columns 'Type', 'Field', 'Value', and 'Actions'. A row is selected with 'Selected' checked, 'eventtype' checked, 'Value' as 'nix-all-logs', and 'Actions' as 'Edit Tags' (highlighted with a green box). A modal window titled 'Create Tags' is open, showing a 'Field Value' of 'eventtype=web\_error' and a 'Tag(s)' field containing 'error, web' (highlighted with a green box). A green arrow points from the 'Edit Tags' button in the main window to the 'Tag(s)' field in the modal.

# Event Types vs. Saved Reports

---

## Event Types

- Categorize events based on a search string
- Used to categorize events into groups
- Inspects incoming events to see if they match a set of criteria
- The eventtype field can be included in a search string
- Does not include a time range

## Saved Reports

- Search criteria do not change
- Can be shared with Splunk users and added to dashboards
- Includes a time range and formatting of the results

# Create Event Types Lab Exercise

---

Time: 10 minutes

Tasks:

- Log into Splunk and configure the instance
- Create an event type for status errors

# Create Workflow Actions

# Topic Objectives

---

- Identify what are workflow actions
- Create a GET, POST, and search workflow action
- Test workflow actions

# What are Workflow Actions?

- Workflow actions allow the user to interact with web resources directly from events and fields present in the search results
  - GET: retrieve information from an external resource
  - POST: send field values to an external resource
  - Search: use field values to perform a secondary search

The screenshot shows a Splunk search results page. An event is selected, displaying its timestamp (4/6/19 10:28:56.817 PM), source (1554589736.817), and type (TCP\_REFRESH\_HIT/200). The event details show a user (tzielinski@buttercupgames.com) performing a GET request to http://www.fftimes.com/themes/fftimes2009/icons/rrr.png. The event has a status of DIRECT and is associated with a file (image/png) and a default case (DefaultGroup-Demo\_Clients-NONE-NONE-DefaultRouting). The event also contains links to news items (IW\_news, ns, etc.) and a link back to the source page.

Event Actions ▾

Build Event Type	Value	Actions
Get info for IP:95.130.170.231	nix-all-logs	▼
Extract Fields	cisco_router1	▼
Show Source	/opt/log/cisco_router1/cisco_ironport_web.log	▼

# Create a GET Workflow Action

Settings > Fields > Workflow Actions > **New Workflow Action**

- ① Select the Destination app
- ② Name the workflow action (no spaces or special characters)
- ③ Define the Label
- ④ Determine if your workflow action applies to a field or event type

The screenshot shows the 'New Workflow Action' configuration page. It includes fields for Destination app, Name, Label, and application rules.

**Destination app:** search 1

**Name \***: get\_whois\_info 2  
Enter a unique name without spaces or special characters later on within Splunk Settings.

**Label \***: Get info for IP:\$src\$ 3  
Enter the label that appears for this action. Optionally in dollar signs, e.g. 'Search for ticket number \$ticket\$'

**Apply only to the following fields**: src\_ip 4  
Specify a comma-separated list of fields that must be in it. When fields are specified, the workflow action only appears in all field menus.

**Apply only to the following event types**:  
Specify a comma-separated list of event types that a to apply to it.

# Create a GET Workflow Action (cont.)

- 5 From the Show action in drop-down list, select Event menu, Fields menu, or Both
- 6 From Action type drop-down list, select link
- 7 Enter the URI of where the user will be directed
- 8 Specify if the link should open in a New window or Current window
- 9 Set Link method to get
- 10 Save

Show action in **Event menu** 5

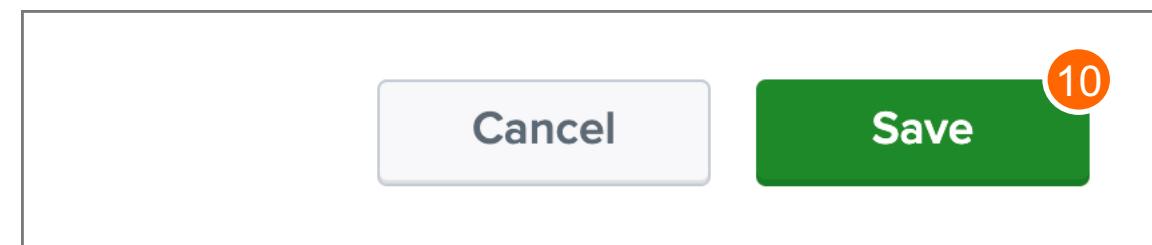
Action type \* **link** 6

**Link configuration**

7 URI \* **https://who.is/whois-ip/ip-address/\$src\_ip\$**  
Enter the location to link to. Optionally, specify fields  
`http://www.google.com/search?q=$host$`

Open link in **New window** 8

Link method **get** 9



# Test the GET Workflow Action

The image shows two screenshots illustrating the use of a GET workflow action in Splunk.

**Splunk Interface Screenshot:**

- A log event table with one entry: "Fri Jun 10 2022 16:55:32 www1 sshd[1595]: Failed password from 91.214.92.22 port 3688 ssh2".
- An "Event Actions" dropdown menu is open, showing options: "Build Event Type", "Get info for IP:", "Extract Fields", and "Show Source".
- The "Get info for IP:" option is highlighted with a green border and has a green arrow pointing to the RIPE Whois results page.
- Below the dropdown, there is a checkbox labeled "src\_ip" followed by the value "91.214.92.22".

**RIPE Whois Database Screenshot:**

## 91.214.92.22 address profile

**Whois Diagnostics**

### IP Whois

NetRange:	91.0.0.0 – 91.255.255.255
CIDR:	91.0.0.0/8
NetName:	91-RIPE
NetHandle:	NET-91-0-0-0-1
Parent:	( )
NetType:	Allocated to RIPE NCC
OriginAS:	
Organization:	RIPE Network Coordination Centre (RIPE)
RegDate:	2005-06-30
Updated:	2009-05-18
Comment:	These addresses have been further assigned to users in
Comment:	the RIPE NCC region. Contact information can be found in
Comment:	the RIPE database at <a href="http://www.ripe.net/whois">http://www.ripe.net/whois</a>
Ref:	<a href="https://rdap.arin.net/registry/ip/91.0.0.0">https://rdap.arin.net/registry/ip/91.0.0.0</a>

# Create a POST Workflow Action

Settings > Fields > Workflow Actions > **New Workflow Action**

Complete steps 1 – 6 as described in the previous example for creating a GET workflow action

The screenshot shows the 'New Workflow Action' configuration page. The fields and their descriptions are:

- Destination app:** search (Step 1)
- Name \***: Create accounting system ticket (Step 2)  
Enter a unique name without spaces or special characters. later on within Splunk Settings.
- Label \***: Open accounting ticket for transaction \$TransactionID\$ (Step 3)  
Enter the label that appears for this action. Optionally, incor in dollar signs, e.g. 'Search for ticket number : \$ticketnum\$'.
- Apply only to the following fields:** result (Step 4)  
Specify a comma-separated list of fields that must be present it. When fields are specified, the workflow action only appears in all field menus.
- Apply only to the following event types:** (Step 5)  
Specify a comma-separated list of event types that an event to apply to it.
- Show action in:** Event menu (Step 5)
- Action type \***: link (Step 6)

# Create a POST Workflow Action (cont.)

- 7 Enter the URI of where the user will be directed
- 8 Open the link in a New window or Current window
- 9 Select the Link method of post
- 10 Provide post argument parameters
- 11 Save

Link configuration

URI \*  7  
Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs.  
`http://www.google.com/search?q=$host$`

Open link in  8

Link method  9

Post arguments

details	= \$_raw\$
environment	= \$host\$
occurred	= \$_time\$
priority	= Urgent
summary	= sales transaction error on \$host\$

+ Add another field

11

# Test the POST Workflow Action

6/10/22 Fri Jun 10 2022 16:57:00 ecomm engine response TransactionID=103529 CustomerID=5i31kp  
4:57:00.000 PM k5 error

Event Actions ▾

- Open accounting ticket for transaction 103529
- Build Event Type
- Extract Fields
- Show Source

Value

- ecommsv1
- /opt/log/ecommsv1/sales\_
- sales\_entries**
- 5i31kpk5

TransactionID ▾ 103529

The diagram illustrates the workflow for creating a bug ticket. On the left, a Splunk event is shown with a timestamp of 6/10/22 at 4:57:00 PM, a source of 'k5 error', and a transaction ID of 103529. An 'Event Actions' dropdown menu is open, with the 'Open accounting ticket for transaction 103529' option selected and highlighted in green. To the right, a 'Bug Tracker 4000' interface is displayed, featuring the Buttercup Games logo. The ticket summary is 'Ticket Added:' with details: 'Ticket Summary: sales transaction error on ecommsv1', 'Priority: Urgent', 'Time of Occurrence: 1654880220', 'Environment: ecommsv1', 'Details: Fri Jun 10 2022 16:57:00 ecomm engine response TransactionID=103529 CustomerID=5i31kpk5 error'. A green arrow points from the 'sales\_entries' value in the Splunk event to the 'Ticket Added:' section of the bug tracker.

Bug Tracker 4000

Ticket Added:

Ticket Summary: sales transaction error on ecommsv1

Priority : Urgent

Time of Occurrence : 1654880220

Environment : ecommsv1

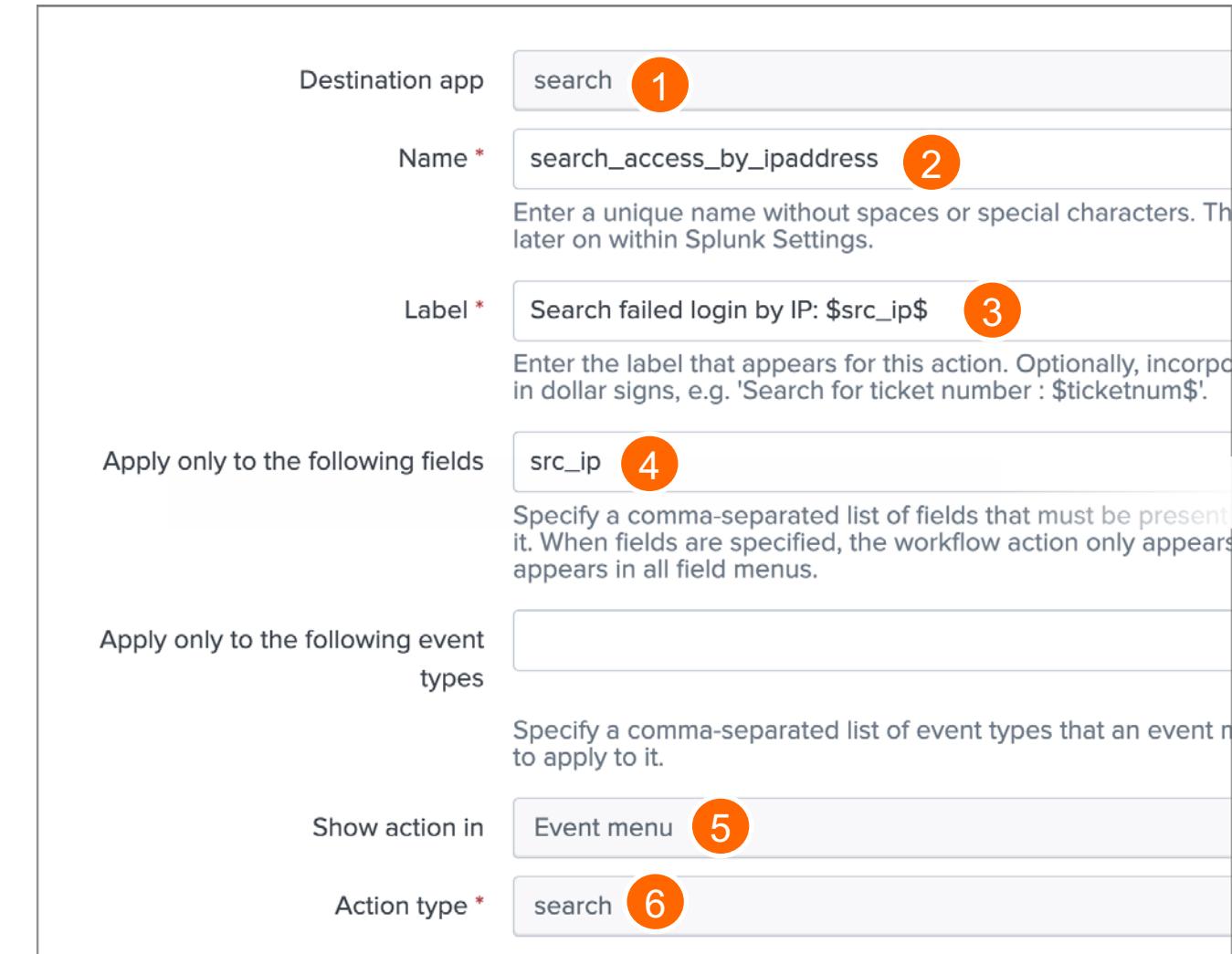
Details : Fri Jun 10 2022 16:57:00 ecomm engine response  
TransactionID=103529 CustomerID=5i31kpk5 error

# Create a Search Workflow Action

Settings > Fields > Workflow Actions > **New Workflow Action**

Complete steps 1 – 5 as described in the previous example for creating a GET workflow action

- ⑥ From the Action type drop-down list, choose search



Destination app **search** 1

Name \* **search\_access\_by\_ipaddress** 2  
Enter a unique name without spaces or special characters. This later on within Splunk Settings.

Label \* **Search failed login by IP: \$src\_ip\$** 3  
Enter the label that appears for this action. Optionally, incorporate dollar signs, e.g. 'Search for ticket number : \$ticketnum\$'.

Apply only to the following fields  
**src\_ip** 4  
Specify a comma-separated list of fields that must be present in it. When fields are specified, the workflow action only appears in all field menus.

Apply only to the following event types  
  
Specify a comma-separated list of event types that an event must have to apply to it.

Show action in **Event menu** 5

Action type \* **search** 6

# Create a Search Workflow Action (cont.)

- 7 Enter the Search string
- 8 Enter the view name where the search will execute
- 9 Indicate if the search should run in a **New window** or the **Current window**
- 10 Set time range options
- 11 Save

Search configuration

7 Search string \* index=security sourcetype=linux\_secure failed src\_ip=\$src\_ip\$  
Enter the search for this action. Optionally, specify fields as \$fieldname\$, controller=\$controller\$ error=\*

Run in app search  
Choose an app for the search to run in. Defaults to the current app.

8 Open in view  
Enter the name of a view for the search to open in. Defaults to the current view.

Run search in New window 9  
Run search in New window

Time range

10 Earliest time  
Latest time  
 Use the same time range as the search that created the field listing

Cancel Save 11

# Test the Search Workflow Action

The screenshot shows the Splunk interface with a search workflow action open. On the left, a sidebar displays a list of actions: 'Build Event Type', 'Get info for IP:', 'Extract Fields', 'Search failed login by IP: 198.35.2.120' (highlighted with a green box), 'Show Source', and 'Event Actions'. Below this is a table of selected fields:

Type	Field	Value
Selected	host	mailsv1
	source	/opt/log mailsv1
	sourcetype	linux_secure
	src_ip	198.35.2.120
Event	action	failure

A green arrow points from the 'Search failed login by IP: 198.35.2.120' action to the search bar in the main search interface. The search bar contains the query: `index=security sourcetype=linux_secure failed src_ip=198.35.2.120`. The main search results show 5 events found between June 9, 2022, and June 10, 2022. The first event is detailed below:

**Event**

i	Time	Event
>	6/10/22 6:28:11.000 PM	Fri Jun 10 2022 18:28:11 mailsv1 sshd[1634]: Failed password for invalid user jabber f rom 198.35.2.120 port 2683 ssh2 host = mailsv1   source = /opt/log/mailsv1/secure.log   sourcetype = linux_secure src_ip = 198.35.2.120
>	6/10/22 6:27:54.000 PM	Fri Jun 10 2022 18:27:54 mailsv1 sshd[1714]: Failed password for invalid user proxy fr om 198.35.2.120 port 2815 ssh2 host = mailsv1   source = /opt/log/mailsv1/secure.log   sourcetype = linux_secure src_ip = 198.35.2.120

# Create Workflow Actions Lab Exercise

---

Time: 15 minutes

Tasks:

- Create a GET workflow to track external login attempts
- Create a POST workflow action that creates an IT ticket in an external system
- Create a Search workflow that performs a search for all failed password events associated with a specific IP address

# Create Tags and Aliases

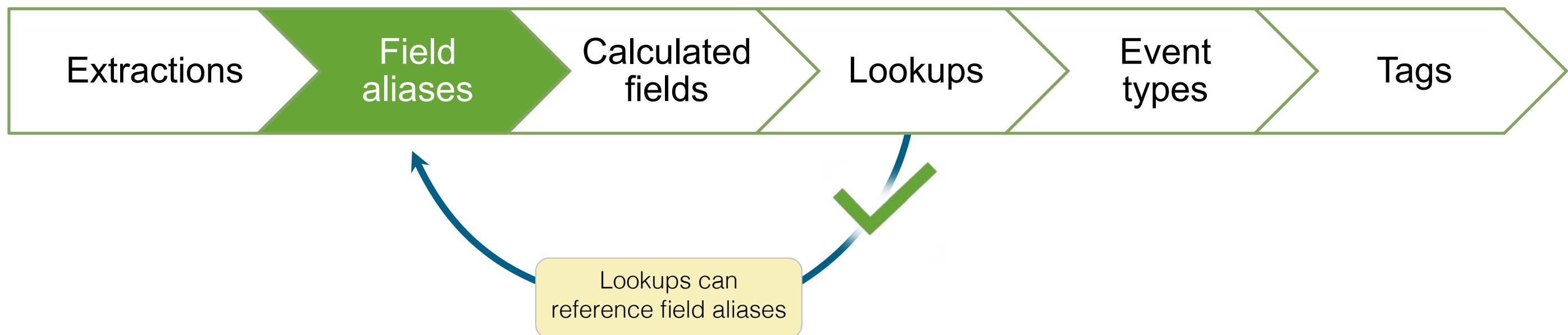
# Topic Objectives

---

- Define field aliases
- Create field aliases
- Search with field aliases
- Define tags
- Create and view tags
- Search with tags
- Manage tags

# Define Field Aliases

- A way to associate an additional (new) name with an existing field name, like a nickname
- Field aliases can be used to normalize field names
- Can be referenced by knowledge objects that succeed aliases in the search process pipeline



# Field Alias Example

- Several source types contain some type of a username field
- To make data correlation and searching easier, normalize the Username and user fields

sourcetype=cisco\_firewall

Selected	<input checked="" type="checkbox"/> host	cisco_router1
	<input checked="" type="checkbox"/> source	/opt/log/cisco_router1/cisco_firewall.log
	<input checked="" type="checkbox"/> sourcetype	cisco_firewall
Event	<input type="checkbox"/> Duration	9h:21m:4s
	<input type="checkbox"/> Group	buttercupgames
	<input type="checkbox"/> IP	10.3.10.241
	<input type="checkbox"/> Username	dhale
	<input type="checkbox"/> bcg_ip	10.3.10.241
	<input type="checkbox"/> bcg_workstation	BG03-dhale

sourcetype=winauthentication\_security

<input type="checkbox"/> ComputerName	BG03-dhale
<input type="checkbox"/> EventCode	4634
<input type="checkbox"/> EventType	8
<input type="checkbox"/> Name	Security
<input type="checkbox"/> Page	Successful
<input type="checkbox"/> SidNumber	9787
<input type="checkbox"/> Sid	S-1-5-21-57989841-920026266-725345543-6444
<input type="checkbox"/> SidType	1
<input type="checkbox"/> SourceName	Security
<input type="checkbox"/> Type	Success
<input type="checkbox"/> User	dhale

To search for all events involving the user dhale, you would have to search for:  
**Username=dhale OR User=dhale**

# Create a Field Alias

Settings > Fields > Field aliases > **New Field Alias**

- ① Select Destination app for field alias
- ② Enter a Name for the field alias (not for searching)
- ③ Choose which host, source, or sourcetype the field alias will be applied to
- ④ Enter existing field name and its new alias

The screenshot shows the 'New Field Alias' configuration page. The 'Destination app' is set to 'search' (1). The 'Name' is 'cisco\_firewall\_aliases' (2). Under 'Apply to', 'sourcetype' is selected (3). In the 'Field aliases' section (4), there is one entry: 'Username' is mapped to 'user'. A green arrow points from 'Username' to 'Field in events', another from 'user' to 'Field alias', and a third from 'Field in events' to 'Field alias'. A checkbox for 'Overwrite field values' is checked. At the bottom right are 'Cancel' and 'Save' buttons.

# Create a Field Alias (cont.)

Settings > Fields > Field aliases > **New Field Alias**

## 5 Overwrite field values affects the behavior of a field alias

- If checked:
  - If user already exists, Splunk replaces user values with Username values
  - If Username doesn't exist or has no value, Splunk removes user from results
- If unchecked, no fields values are

The screenshot shows the 'New Field Alias' configuration page. The 'Destination app' is set to 'search'. The 'Name' is 'cisco\_firewall\_aliases'. Under 'Apply to', 'sourcetype' is selected, and 'named' is set to 'cisco\_firewall'. In the 'Field aliases' section, there is one entry: 'Username' = 'user'. Below this is a button '+ Add another field'. At the bottom left is a checked checkbox labeled 'Overwrite field values' with a red circle containing the number 5. At the bottom right are 'Cancel' and 'Save' buttons, with the 'Save' button being green and having a red circle containing the number 6.

## 6 Save

# Create a Field Alias (cont.)

New field alias required for each sourcetype

The screenshot shows two parallel configuration panels for creating field aliases.

**Left Panel (Top):**

- Destination app: search
- Name \*: cisco\_firewall\_aliases
- Apply to: sourcetype (dropdown), named \*: cisco\_firewall (highlighted)
- Field aliases: Username = user (highlighted with a green box)
- + Add another field
- Overwrite field values

**Right Panel (Bottom):**

- Destination app: search
- Name \*: winauthentication\_security\_aliases
- Apply to: sourcetype (dropdown), named \*: winauthentication\_security (highlighted)
- Field aliases: User = user (highlighted with a green box)
- + Add another field
- Overwrite field values
- Delete
- Cancel
- Save

# Search with Field Alias: Testing

After the field alias is created, perform a search using the new field alias

New Search

user=dhale\*

212 events (4/5/20 6:00:00.000 PM to 4/12/20 6:53:45.000 PM) No Event Sampling Job Smart Mode

Last 7 days

Events (212) Patterns Statistics Visualization

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

List Format 20 Per Page

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

< Hide Fields All Fields

SELECTED FIELDS

- a eventtype 3
- a host 2
- a source 3
- a sourcetype 3**

INTERESTING FIELDS

- a action 3
- a bcg\_ip 1
- a bcg\_workstation 1
- # bytes\_in 100+
- a c\_ip 100+
- a cc\_method 1

**sourcetype**

3 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

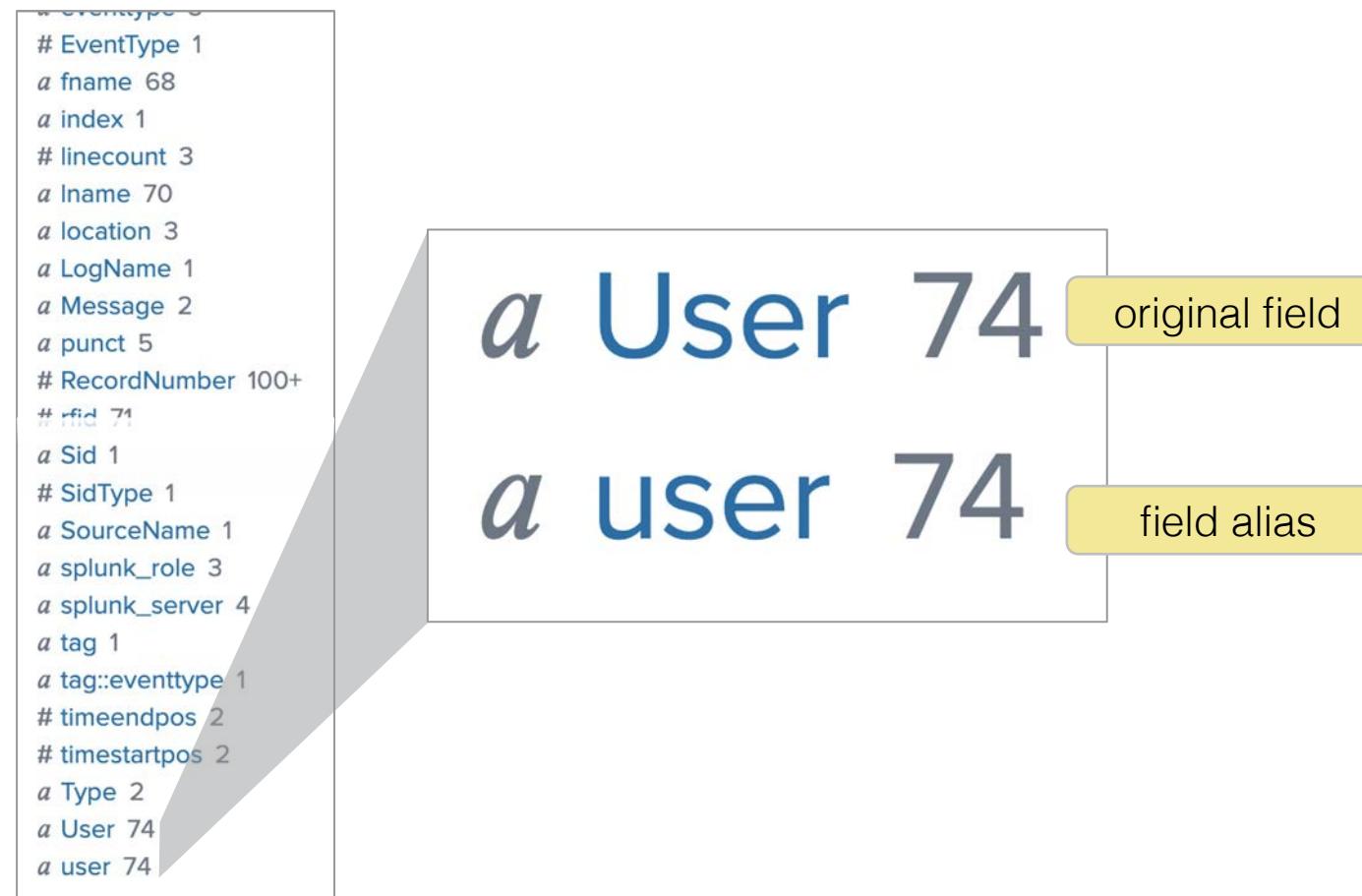
Values

	Count	%
cisco_wsa_squid	193	91.038%
winauthentication_security	17	8.019%
cisco_firewall	2	0.943%

/www.myspace.c  
DEFAULT\_CASE-D  
,0,-,-,-,-,0,  
  
http://www.pho  
.com DIRECT/ww  
NONE-NONE-Defa  
.phones.com/

# Search with Field Aliases: Original Fields

- When you create a field alias, the original field is not affected
- Both fields appear in the All Fields and Interesting Fields lists, if they appear in at least 20% of events



# Search with Field Aliases: Lookups

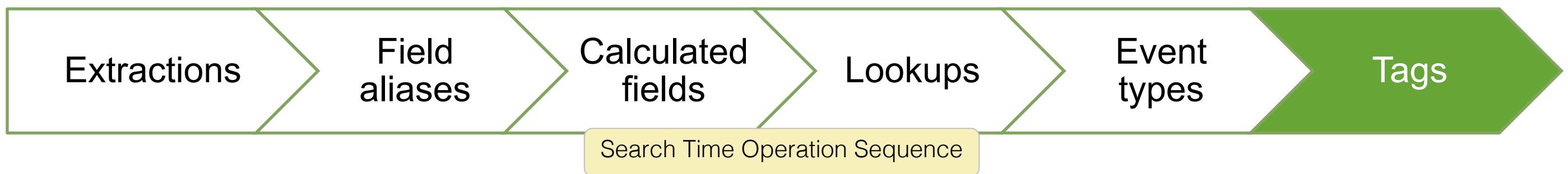
After you have defined your field aliases, you can reference them in a lookup table

The screenshot shows the 'Field Alias' configuration screen in Splunk. The 'Destination app' is set to 'search', the 'Name' is 'cisco\_firewall\_aliases', and it is applied to 'sourcetype'. A 'named' lookup named 'cisco\_firewall' is selected. In the 'Field aliases' section, 'Username' is aliased to 'user'. Below the interface, a terminal window displays a CSV file named 'employees.csv' containing employee data. The 'user' field in the CSV is highlighted with a green box, matching the alias definition.

rfid	fname	lname	user	email	dept	location	ip	hostname	splunkrole
736098118591	Ester	Williams	ewilliams	ewilliams@buttercupgames.com	CIO	SanFrancisco	10.1.10.133	BG01-ewilliams	power
742522500628	Mizuhito	Kemmerer	mkemmerer	mkemmerer@buttercupgames.com	Compensation and Benefits	Boston	10.2.10.3	BG02-mkemmerer	user
464056218740	Mori	Yavatkar	myavatkar	myavatkar@buttercupgames.com	Compensation and Benefits	SanFrancisco	10.1.10.140	BG01-myavatkar	user
139089031800	Gogol	Bowser	gbowser	gbowser@buttercupgames.com	Compensation and Benefits	London	10.3.10.22	BG03-gbowser	user
227128834140	David	Johnson	djohnson	djohnson@buttercupgames.com	Compliance	SanFrancisco	10.3.10.180	BG02-djohnson	power
675871244218	Saran	Wrappe	swrappe	swrappe@buttercupgames.com	Corporate Counsel	SanFrancisco	10.1.10.188	BG01-swrappe	user
791183986583	Patricia	dAbbeville	pdabbeville	pdabbeville@buttercupgames.com	Documentation	SanFrancisco	10.1.10.52	BG01-pdabbeville	user
632071692298	Yanto	Owen	yowen	gra@buttercupgames.com	Documentation	London	10.2.10.170	BG03-yowen	user
559129672655	Enrique	Dutra	edutra	edutra@buttercupgames.com	Engineering	Boston	10.2.10.77	BG02-edutra	power
382839148784	Meng	Yuan	myuan	myuan@buttercupgames.com	Engineering	SanFrancisco	10.1.10.238	BG01-myuan	power
356025036673	Guoxiang	Nooteboom	gnooteboom	gnooteboom@buttercupgames.com	Engineering	SanFrancisco	10.1.10.12	BG01-gnooteboom	power
569361105570	Kathleen	Percy	kpercy	kpercy@buttercupgames.com	Engineering	SanFrancisco	10.1.10.216	BG01-kpercy	power

# Define Tags

- A knowledge object that enables you to search for events that contain specific field/value combinations
- Tags are labels that you create for field/value pairs
- Tags make your data more understandable and less ambiguous
- Any field/value combination can be referenced by more than one tag and any tag can be applied to more than one field/value pair
- Tags are case sensitive



# Create Tags

- 1 Click the info arrow for event details
- 2 Under Actions, click the down arrow (fields menu)
- 3 Select Edit Tags
- 4 Enter the Tag labels associated with this key/value pair separated by commas
- 5 Save

The screenshot shows the Splunk interface for creating tags. At the top, there is an event details panel with a timestamp (6/10/22, 7:06:57.000 PM) and an event message (Fri Jun 10 2022 19:06:57 www1 sshd[10370]: Accepted password for nsharpe from 10.2.1 0.163 port 3115 ssh2). Below this is a table of selected fields:

Type	Field	Value	Actions
Selected	host	www1	<input type="button" value="Edit Tags"/> (highlighted with a green box and orange circle)
	source	/opt/log/www1/se	<input type="button" value="Edit Tags"/>
	sourcetype	linux_secure	<input type="button" value="Edit Tags"/>
	src_ip	10.2.10.163	<input type="button" value="Edit Tags"/>
Event	action	success	<input type="button" value="Edit Tags"/>

A dropdown menu is open over the 'Edit Tags' button, with the option 'Edit Tags' highlighted with a green box and orange circle.

A modal window titled 'Create Tags' is open at the bottom. It contains a 'Field Value' input field with 'host=www1' and a 'Tag(s)' input field with 'webserver, production, sf'. A note below says 'Comma or space separated list of tags.' At the bottom right of the modal are 'Cancel' and 'Save' buttons, with the 'Save' button highlighted with a green box and orange circle.

# View Tags

- When tagged field/value pairs are selected, the tags appear
  - A In the results as tags
  - B In parentheses next to the associated field/value pair

The screenshot shows a Splunk search results page. At the top, an event is displayed: "6/10/22 Fri Jun 10 2022 19:31:51 www1 sshd[2684]: Failed password for invalid user henri from 10.1.10.172 port 2506 ssh2". Below the event, the raw log data is shown: "host = www1 production sf webserver | sourcetype = linux\_secure | src\_ip = 10.1.10.172 | tag = production tag = sf tag = webserver". A green box highlights this raw data, and a red circle labeled 'A' is placed over the word "tag". To the right, a detailed view of the selected tags is shown in a table:

Type	Field	Value	Actions
Selected	host	www1 (production sf webserver)	▼
	source	/opt/log/www1/secure.log	▼
	sourcetype	linux_secure	▼
	src_ip	10.1.10.172	▼
Event	action	failure	▼
	app	sshd	▼
	dest	www1	▼
	pid	2684	▼
	process	sshd	▼
	src_port	2506	▼
	ssh_protocol	ssh2	▼
	tag	production	▼
		sf	▼
		webserver	▼
	user	henri	▼

A red circle labeled 'B' is placed over the value "www1 (production sf webserver)" in the first row of the table.

# Search for Tags

A tag associated with a value:

`tag=<tagnname>``tag=webserver`

A tag using a partial field value:

`tag=<partial-tagnname>*``tag=w*`

A tag associated with a value on a specific field:

`tag::<field>=<tagnname>``tag::host=webserver`

# Use Tags in a Search

New Search

Save As ▾ Create Table View Close

```
index=security sourcetype=linux_secure tag=webserver src_ip!=NULL  
| stats count by src_ip, host
```

Last 24 hours ▾ 

✓ 428 events (6/9/22 7:00:00.000 PM to 6/10/22 7:40:38.000 PM) No Event Sampling ▾ Job ▾  Smart Mode ▾

Events Patterns Statistics (35) Visualization

20 Per Page ▾  Preview ▾ < Prev 1 2 Next >

src_ip	host	count
10.1.10.172	www1	57
10.2.10.163	www1	37
10.3.10.46	www1	52
108.65.113.83	www1	12
110.138.30.229	www1	15
125.7.55.180	www1	4
148.107.2.20	www1	21

# Manage Tags: Permissions / Status

Settings > Tags > List by field value pair

- A Edit permissions
- B Disable all tags for the pair: disables the tag in searches and prevents it from being listed under List by Tag Name and All unique tag objects

List by field value pair						<a href="#">New Tag</a>
<a href="#">Tags</a> » List by field value pair						
Showing 1-2 of 2 items						
App	Search & Reporting (s... ▾)	Owner	Any	Visible in the App ▾	filter <input type="text"/>	<input type="button" value="25 per page ▾"/>
Field value pair ▾	Tag name ▾	App ▾	Sharing ▾	Status ▾	Actions	
<a href="#">eventtype=bcg_online_sales</a>	web	ao-bcg-locl	<a href="#">Global   Permissions</a>	Enabled	<a href="#">Clone</a>	
host=www1	production, sf, webserver	search	<a href="#">Private   Permissions</a>	Enabled   <a href="#">Disable all tags for pair</a>	<a href="#">Clone</a>   <a href="#">Move</a>   <a href="#">Delete</a>	

# Manage Tags: Tag Name

Settings > Tags > List by field value pair

Click Field value pair to add additional tags or change the name of the tag

List by field value pair

Tags » List by field value pair

Showing 1-2 of 2 items

App Search & Reporting (s... Owner Any Visibility

Field value pair	Tag name	App	Sharing
eventtype=bcg_online_sales	web	ao-bcg-loc1	Global
host=www1	production, sf, webserver	search	Private

host=www1

Tags » List by field value pair » host=www1

Tag name Enter one tag per textfield

production

sf

webserver

+ Add another field

Cancel Save

A green box highlights the 'host=www1' row in the main table. A green arrow points from the 'host=www1' entry in the main table to the 'host=www1' entry in the modal dialog.

# Create Tags and Aliases Lab Exercises

---

Time: 15 minutes

Tasks:

- Create a field alias for the `cs_username` and `users` fields
- Create a field alias for the `http_action` and `http_method` fields
- Create tags to identify all admin accounts

# Create Search Macros

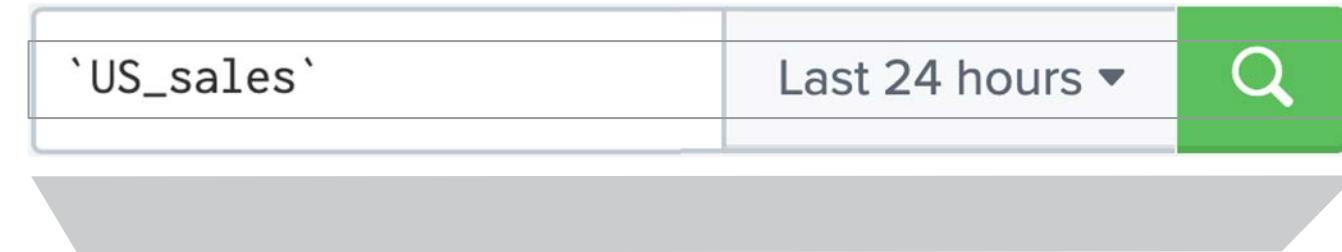
# Topic Objectives

---

- Define macros
- Create macros with and without arguments
- Validate macro arguments
- Use and preview macros at search time
- Use nested macros
- Use macros with other knowledge objects
- Use tags/event types with macros
- Create macros considerations

# Define Macros

- Useful for frequently run searches with similar syntax
- Time range selected at search time
- Can be a full search string or a portion of a search that can be reused in multiple places
- Allows you to define arguments within a search segment and pass parameters at execution time



```
index=sales sourcetype=vendor_sales  
VendorCountry="United States"  
| stats sum(price) as USD by product_name  
| eval USD = "$".tostring(USD, "commas")
```

product_name	USD
Benign Space Debris	\$49.98
Curling 2014	\$99.95
Dream Crusher	\$479.88
Final Sequel	\$49.98
Fire Resistance Suit of Provolone	\$39.90
Holy Blade of Gouda	\$71.88
Manganiello Bros.	\$319.92
Manganiello Bros. Tee	\$79.92
Mediocre Kingdoms	\$149.94

# Create a Macro: Without Arguments

Settings > Advanced Search > Search macros > Add new

- 1 Choose destination app
- 2 Create the macro name that will be used in search
- 3 Test the macro definition, i.e., search string, before creating macro
- 4 Save

1 Destination app

2 Name \*   
Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)

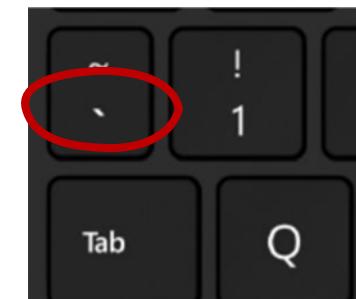
Definition \*   
Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: \$arg1\$  
`index=sales sourcetype=vendor_sales VendorCountry="United States"`

3   
`| stats sum(price) as USD by product_name`  
`| eval USD = $"$.tostring('USD', 'commas')`

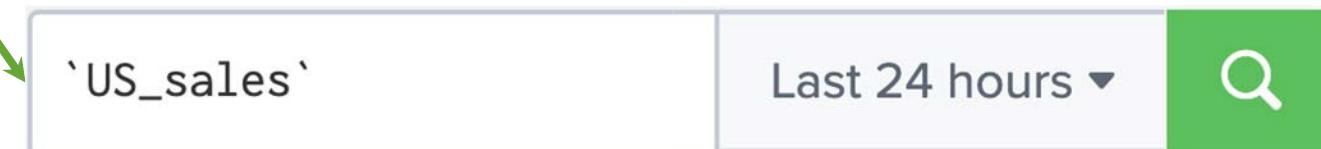
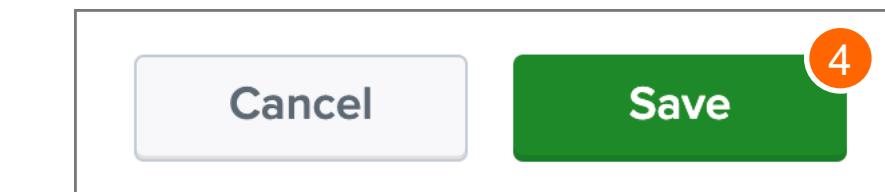
Macros are called to the search line by wrapping the macro name in back ticks



Mac



Windows



# Create a Macro: With Arguments

Settings > Advanced Search > Search macros > Add new

1 monthly\_sales(3)

2 Definition \*

index=sales sourcetype=vendor\_sales VendorCountry="United States"  
| stats sum(price) as USD by product\_name  
| eval \$currency\$ = "\$symbol\$".tostring(round(USD\*\$rate\$,2),"commas"),  
USD="\$".tostring(USD,"commas")

3 Arguments

currency, symbol, rate

Destination app search

Name \* Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)  
monthly\_sales(3)

Definition \* Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: \$arg1\$

Use eval-based definition?

Arguments Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '\_' and '-' characters.

# Validate Macro Arguments

- 4 Define a Validation Expression to verify arguments using eval or boolean expressions
- 5 Create a Validation Error Message to be displayed if arguments fail validation
- 6 Save

The screenshot shows a configuration dialog for validating macro arguments. The steps are numbered 4, 5, and 6, corresponding to the list above.

- Step 4: Validation Expression**  
The 'Arguments' field contains 'currency,symbol,rate'.  
The 'Validation Expression' field contains 'isnum(\$rate\$)'.
- Step 5: Validation Error Message**  
The 'Validation Error Message' field contains 'The 'rate' value must be a number'.
- Step 6: Save**  
A green 'Save' button is highlighted with a red circle containing the number 6.

# Validate Macro Arguments (cont.)

The screenshot shows a 'New Search' window in Splunk. The search bar contains the command `monthly\_sales(euro,€,\$0.79)`. To the right of the search bar are two buttons: 'Last 30 days ▾' and a green search icon. Below the search bar, an error message is displayed: '! Error in 'SearchParser': Encountered the following error while validating macro 'monthly\_sales(euro,€,\$0.79)': The 'rate' value must be a number.' The rest of the interface includes tabs for 'Events' (selected), 'Patterns', 'Statistics', and 'Visualization', and buttons for 'No Event Sampling ▾', 'Smart Mode ▾', 'List ▾', 'Format', '20 Per Page ▾', and view modes 'i' (Info), 'Time', and 'Event'.

# Use Macros with Arguments at Search Time

- Include arguments in parentheses, separated by commas, following the macro name
- Be sure to pass in the arguments in the same order as you listed them when creating macro

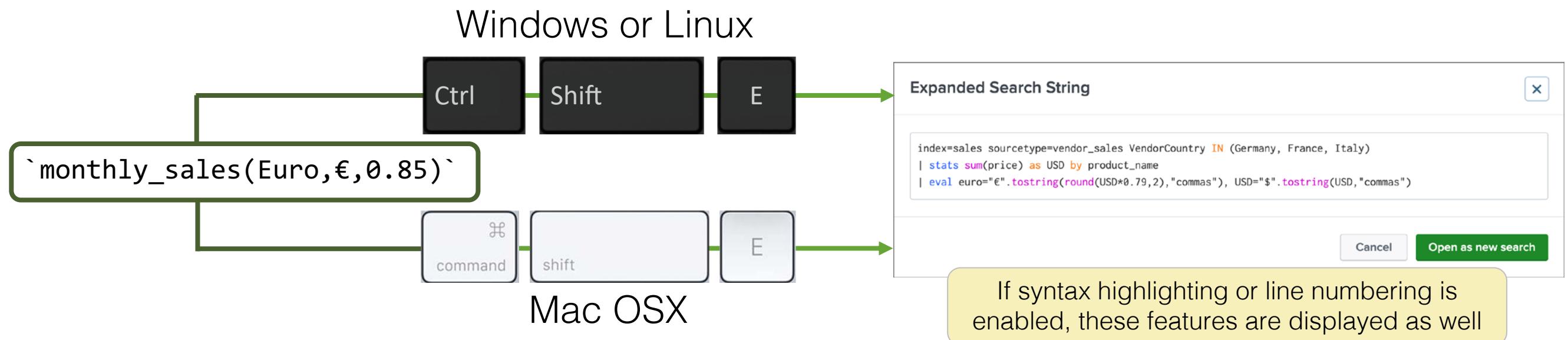
```
`monthly_sales(euro,€,0.79)`
```

```
index=sales sourcetype=vendor_sales  
VendorCountry IN(Germany, France, Italy)  
| stats sum(price) as USD by product_name  
| eval euro="€".toString(round(USD*0.79,2),  
"commas"), USD="$".toString(USD,"commas")
```

product_name	USD	euro
Benign Space Debris	\$1,149.54	€908.14
Curling 2014	\$839.58	€663.27
Dream Crusher	\$919.77	€726.62
Final Sequel	\$374.85	€296.13
Fire Resistance Suit of Provolone	\$227.43	€179.67
Holy Blade of Gouda	\$233.61	€184.55
Manganiello Bros.	\$3,319.17	€2,622.14

# Preview a Macro

To expand search macros, use the keyboard shortcut:



Splunk displays the expanded search string, resolving all nested search macros

Note



You cannot edit in preview.

# Use Nested Search Macros

Macros can be nested within each other

1. Create “inner” macro first
2. Put “inner” macro name surrounded by backticks in definition of “outer” macro

The image consists of two side-by-side screenshots of a Splunk search macro configuration interface.

**Left Screenshot (Inner Macro):**

- Destination app:** class\_Fund3
- Name \***: location\_count
- Definition \***: stats count by location

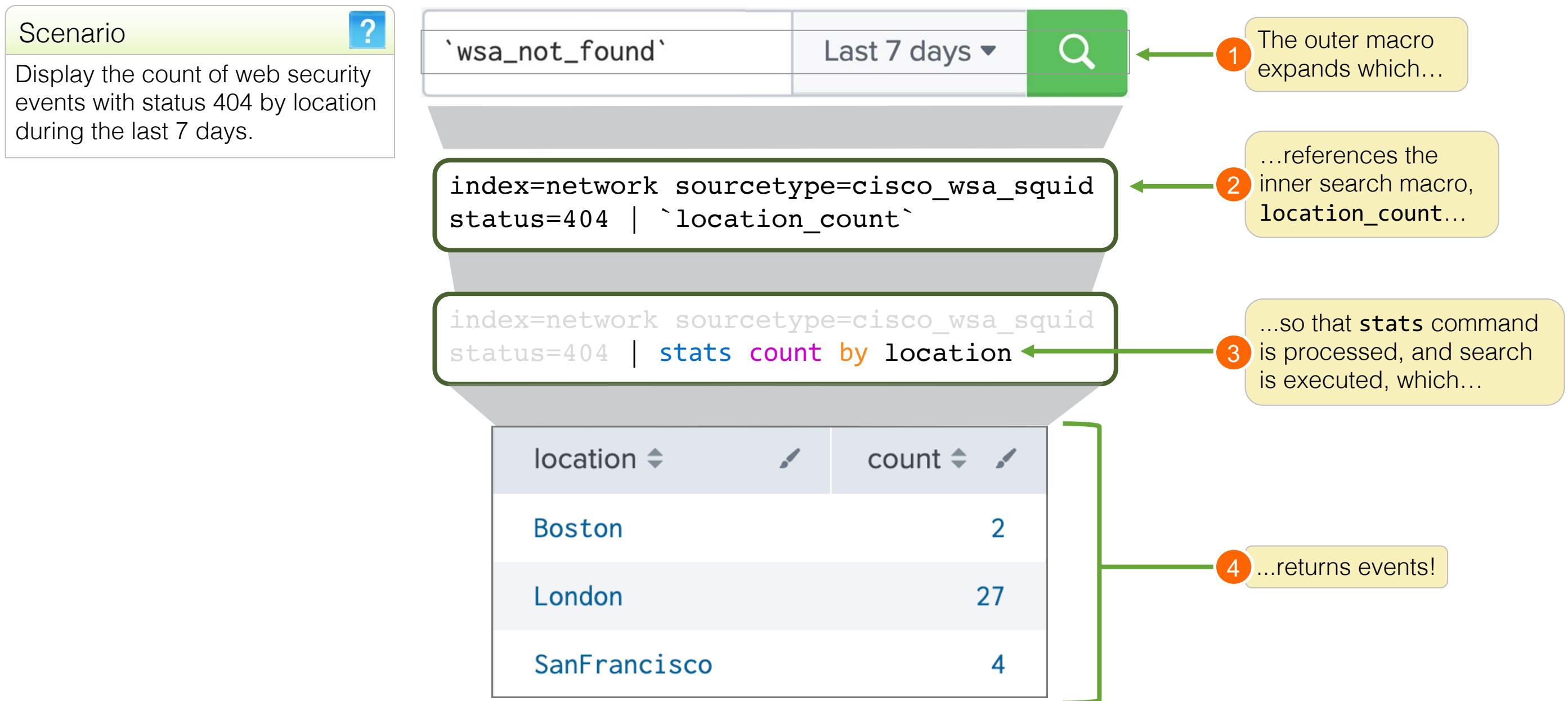
A yellow box labeled "inner macro" highlights the Name field and the Definition field.

**Right Screenshot (Outer Macro):**

- Destination app:** class\_Fund3
- Name \***: wsa\_not\_found
- Definition \***: index=network sourcetype=cisco\_wsa\_squid status=404 |`location\_count`'

A yellow box labeled "outer macro" highlights the Definition field.

# Use Nested Search Macros Example



# Use Nested Search Macros with Arguments

- Arguments can be passed from “outer” macro to “inner” macro
- Provide variable values at search time

The diagram illustrates the configuration of two search macros: an "inner macro" and an "outer macro".

**inner macro:** This macro is defined under the "search" destination app. It has the following fields:

- Name \***: stats\_count(1)
- Definition \***: stats count by \$countfield\$
- Arguments**: countfield

**outer macro:** This macro is also defined under the "search" destination app. It has the following fields:

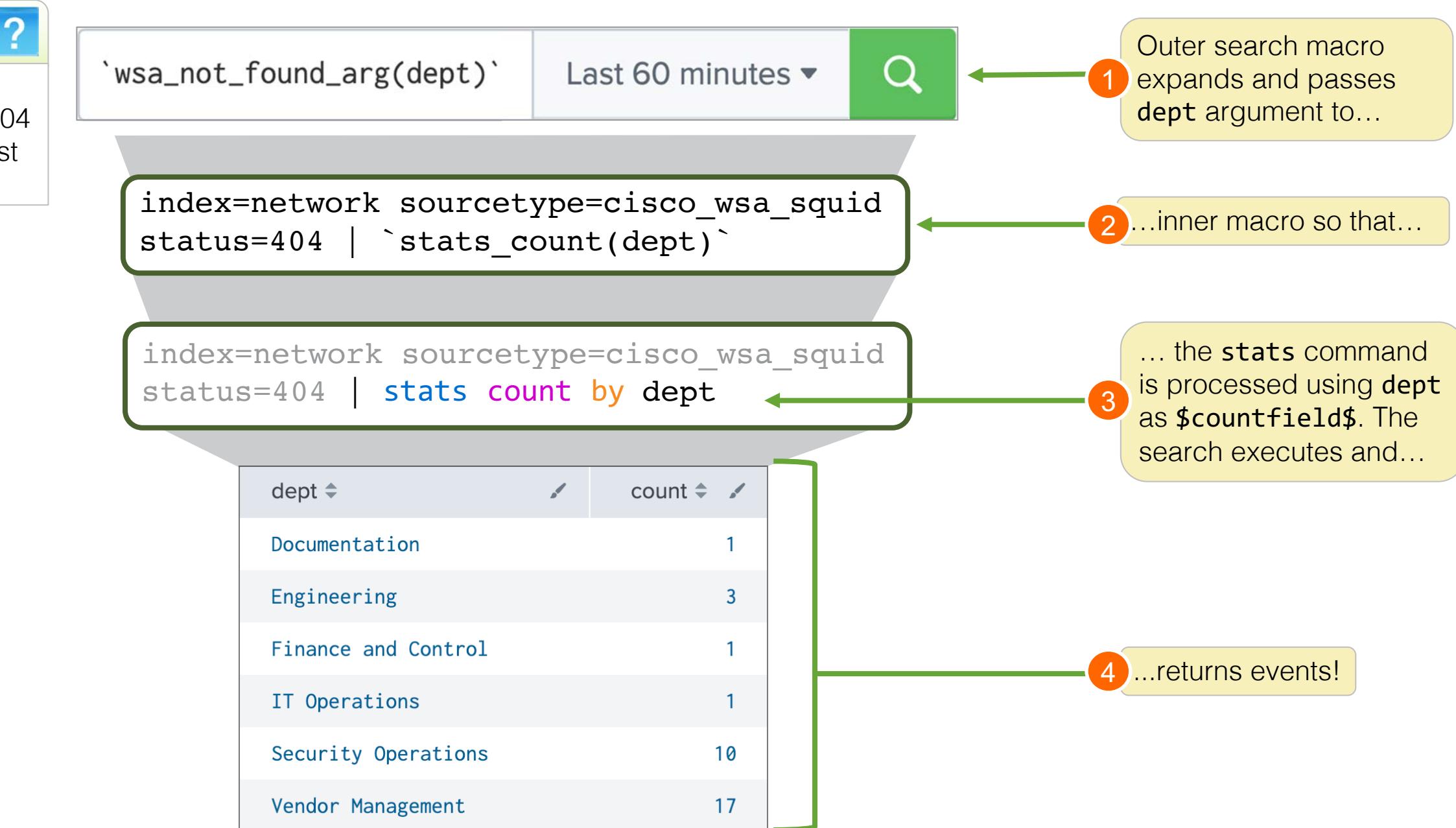
- Name \***: wsa\_not\_found\_arg(1)
- Definition \***: index=network sourcetype=cisco\_wsa\_squid status=404 | `stats\_count(\$countfield\$)`
- Arguments**: countfield

A yellow callout box labeled "inner macro" points to the "Name" field of the inner macro configuration. Another yellow callout box labeled "outer macro" points to the "Name" field of the outer macro configuration.

# Use Nested Search Macros with Arguments (cont.)

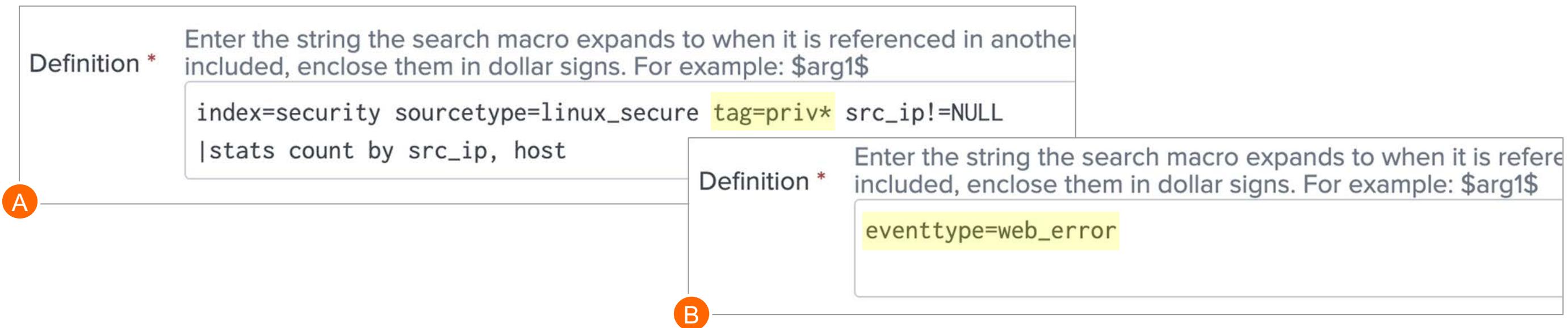
## Scenario

Display the count of web security events with status 404 by department during the last 60 minutes.



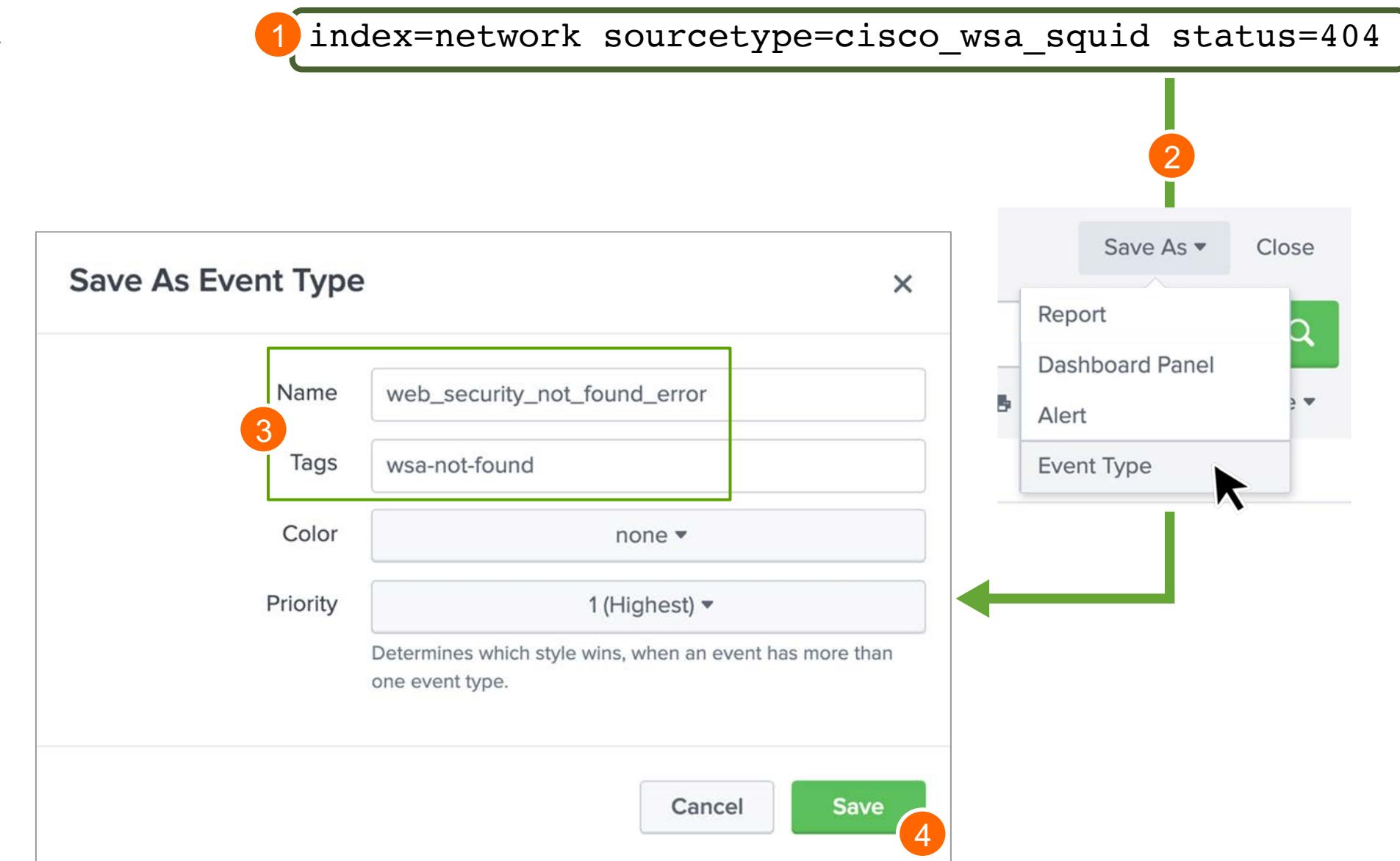
# Use Macros with Other Knowledge Objects

- Ⓐ Reference knowledge objects in macros just as you would from the search bar—field aliases, calculated fields, tags, etc.
- Ⓑ The following slides show how to use tags and event types with macros



# Use Tags/Event Types with Macros

- 1 Run a search and verify that all results meet your event type criteria
- 2 Save As > Event Type
- 3 Provide a Name and optional Tags for your event type
- 4 Save



# Use Tags/Event Types with Macros (cont.)

Settings > Advanced Search > Search macros > Add new

- 1 Choose Destination app
- 2 Enter a name for the macro
- 3 Include the event type OR tag in the macro Definition
- 4 Save

The screenshot shows the 'Add new' search macro configuration dialog. The 'Destination app' is set to 'search'. The 'Name' field contains 'wsa\_not\_found\_loc\_totals'. The 'Definition' field contains 'tag=wsa-not-found | `location\_count`'. The 'Save' button is highlighted with a red circle containing the number 4.

1 Destination app search

Name \* wsa\_not\_found\_loc\_totals

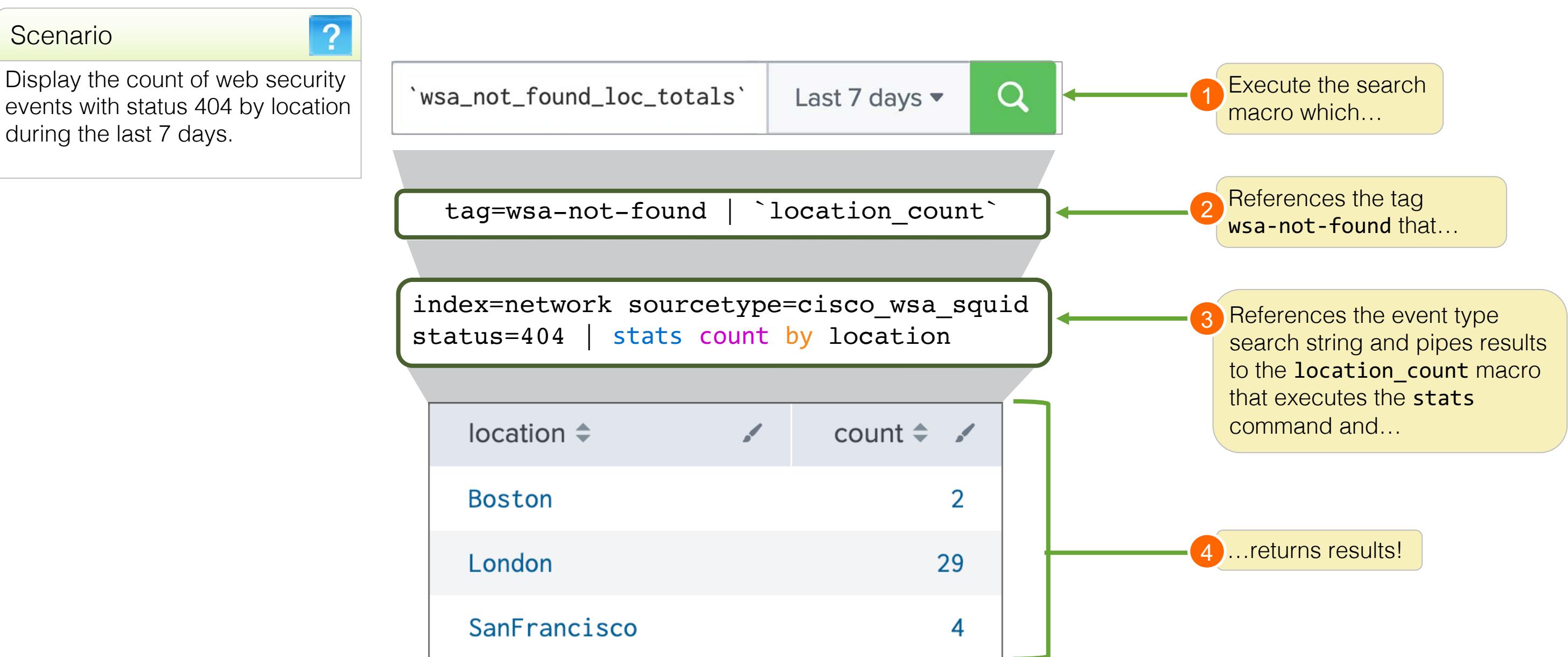
Definition \* tag=wsa-not-found | `location\_count`

Validation Expression

Validation Error Message

Cancel Save 4

# Use Tags/Event Types with Macros (cont.)



# Create Macros: Considerations

---

- When validating more than one argument
  - Use **AND** operator if you want all expressions to be validated
  - The validation error message should be inclusive of all validations
- When creating a macro that begins with a command, don't include a pipe
  - Allow the user to enter the pipe before the macro
  - Avoids having two consecutive pipes, which would give an error

# Create Search Macros Lab Exercise

---

Time: 15 minutes

Tasks:

- Create a macro that will provide a table displaying the total of products in certain European countries
- Use a macro with arguments in a search
- Edit a macro and use the `isnum` function to validate the rate field

# Create Calculated Fields

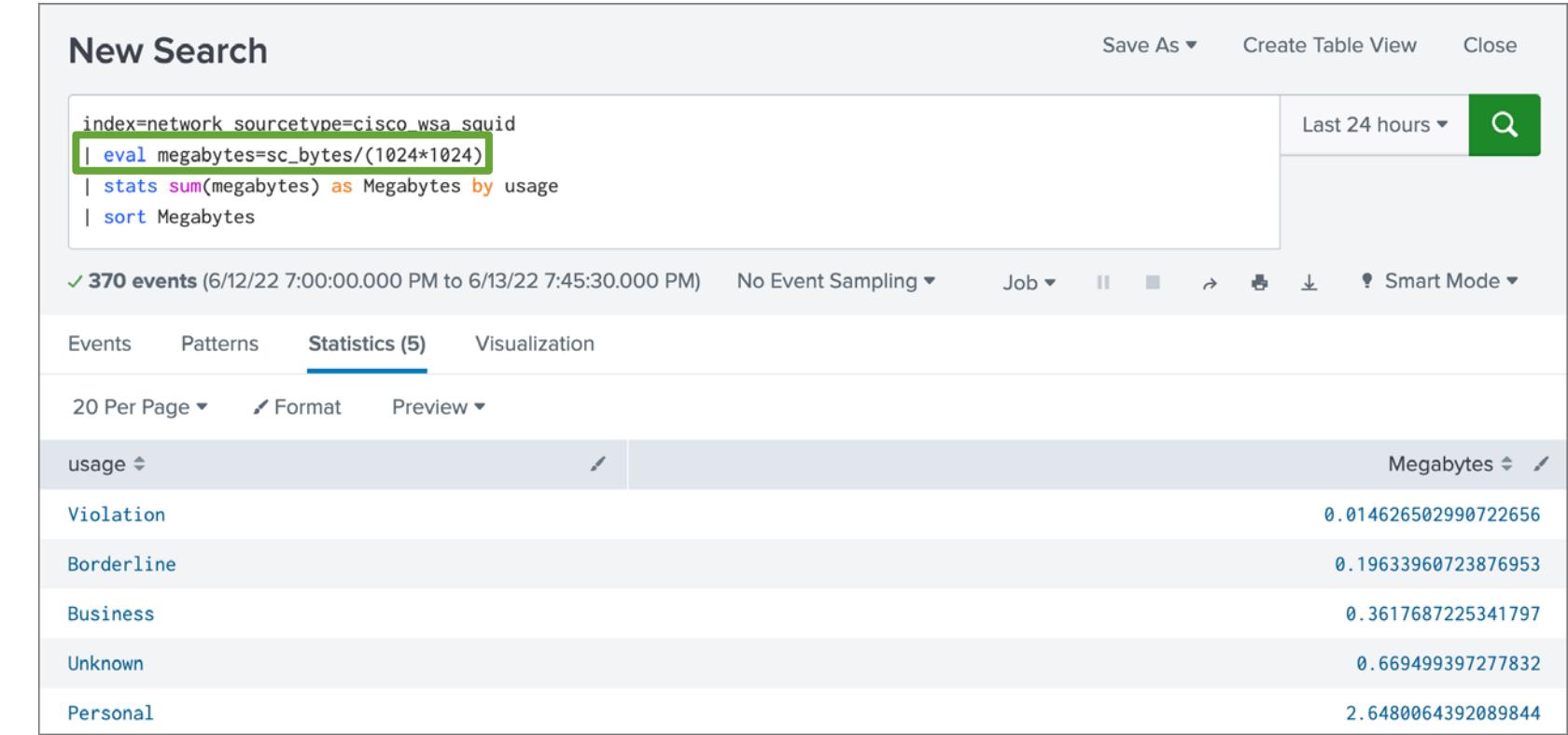
# Topic Objectives

---

- What is a calculated field
- Create a calculated field
- Use a calculated field

# What is a Calculated Field?

- Shortcut for performing repetitive, long, or complex calculations using the `eval` command
- Can only be based on extracted or aliased fields



The screenshot shows the Splunk interface for a "New Search". The search bar contains the following SPL command:

```
index=network sourcetype=cisco_wsa_squid  
| eval megabytes=sc_bytes/(1024*1024)  
| stats sum(megabytes) as Megabytes by usage  
| sort Megabytes
```

The search results table has "usage" as the primary key and "Megabytes" as the secondary key. The data is as follows:

usage	Megabytes
Violation	0.014626502990722656
Borderline	0.19633960723876953
Business	0.3617687225341797
Unknown	0.669499397277832
Personal	2.6480064392089844



# Create a Calculated Field

Settings > Fields > Calculated fields > **New Calculated Field**

- 1 Select the app that will use the calculated field
- 2 Select and specify the **host**, **source**, or **sourcetype** to apply to the calculated field
- 3 Name the calculated field
- 4 Define the **Eval expression**
- 5 Save

1 Destination app: search

2 Apply to: sourcetype, named: cisco\_wsa\_squid

3 Name: megabytes  
Name of the field whose value will be calculated

4 Eval expression: sc\_bytes/(1024\*1024)  
A valid eval expression, e.g. x + 3

Cancel **Save** 5

# Use a Calculated Field

After you have created a calculated field, you can use it in a search like any extracted field

No manual eval is necessary

New Search

```
index=network sourcetype=cisco_wsa_squid  
| stats sum(megabytes) as Megabytes by usage  
| sort Megabytes
```

Last 24 hours 

✓ 379 events (6/12/22 7:00:00.000 PM to 6/13/22 7:54:44.000 PM) No Event Sampling ▾ Job ▾ II ▾ ↗ ▾ Smart Mode ▾

Events Patterns Statistics (5) Visualization

20 Per Page ▾ Format Preview ▾

usage	Megabytes
Violation	0.0146265029907226560
Borderline	0.1963396072387695300
Business	0.3617687225341797000
Unknown	0.6694993972778320000
Personal	2.6771373748779297000

# Create Calculated Fields Lab Exercise

---

Time: 5 minutes

Tasks:

- Create a calculated field that converts bytes to MB

# Wrap-up Slides

# Community

---

- Splunk Community Portal  
[community.splunk.com](https://community.splunk.com)
  - Answers
  - Discussions
  - Splunk Trust
  - User Groups
  - Ideas
- Splunk Blogs  
[splunk.com/blog/](https://splunk.com/blog/)
- Splunk Apps  
[splunkbase.com](https://splunkbase.com)
- Splunk Dev Google Group  
[groups.google.com/forum/#!forum/splunkdev](https://groups.google.com/forum/#!forum/splunkdev)
- Splunk Docs on Twitter  
[twitter.com/splunkdocs](https://twitter.com/splunkdocs)
- Splunk Dev on Twitter  
[twitter.com/splunkdev](https://twitter.com/splunkdev)
- Splunk Live!  
[splunklive.splunk.com](https://splunklive.splunk.com)
- .conf  
[conf.splunk.com](https://conf.splunk.com)

# Support Programs

- **Web**

Documentation: [dev.splunk.com](https://dev.splunk.com) and [docs.splunk.com](https://docs.splunk.com)

Wiki: [wiki.splunk.com](https://wiki.splunk.com)

- **Splunk Lantern**

Guidance from Splunk experts  
[lantern.splunk.com](https://lantern.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](https://splunk.com/index.php/submit_issue)

- **Enterprise, Cloud, ITSI, Security Support**

Web: [splunk.com/en\\_us/about-splunk/contact-us.html#tabs/customersupport](https://splunk.com/en_us/about-splunk/contact-us.html#tabs/customersupport)

Phone: (855) SPLUNK-S or (855) 775-8657

Support ^

**Support Portal**

Submit a case ticket

**Splunk Answers**

Ask Splunk experts questions

**Contact Us**

Contact our customer support

**Product Security Updates**

Keep your data secure

**System Status**

# Learning Paths (cont.)

---

## Knowledge Manager - Recommended Courses

Free eLearning courses are in blue and courses with an \* are present in both learning paths.

- What is Splunk \*
- Introduction to Splunk \*
- Using Fields \*
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Introduction to Dashboards
- Dynamic Dashboards
- Using Choropleth
- Search Optimization \*

# Learning Paths

---

## Search Expert - Recommended Courses

Free eLearning courses are in blue and courses with an \* are present in both learning paths.

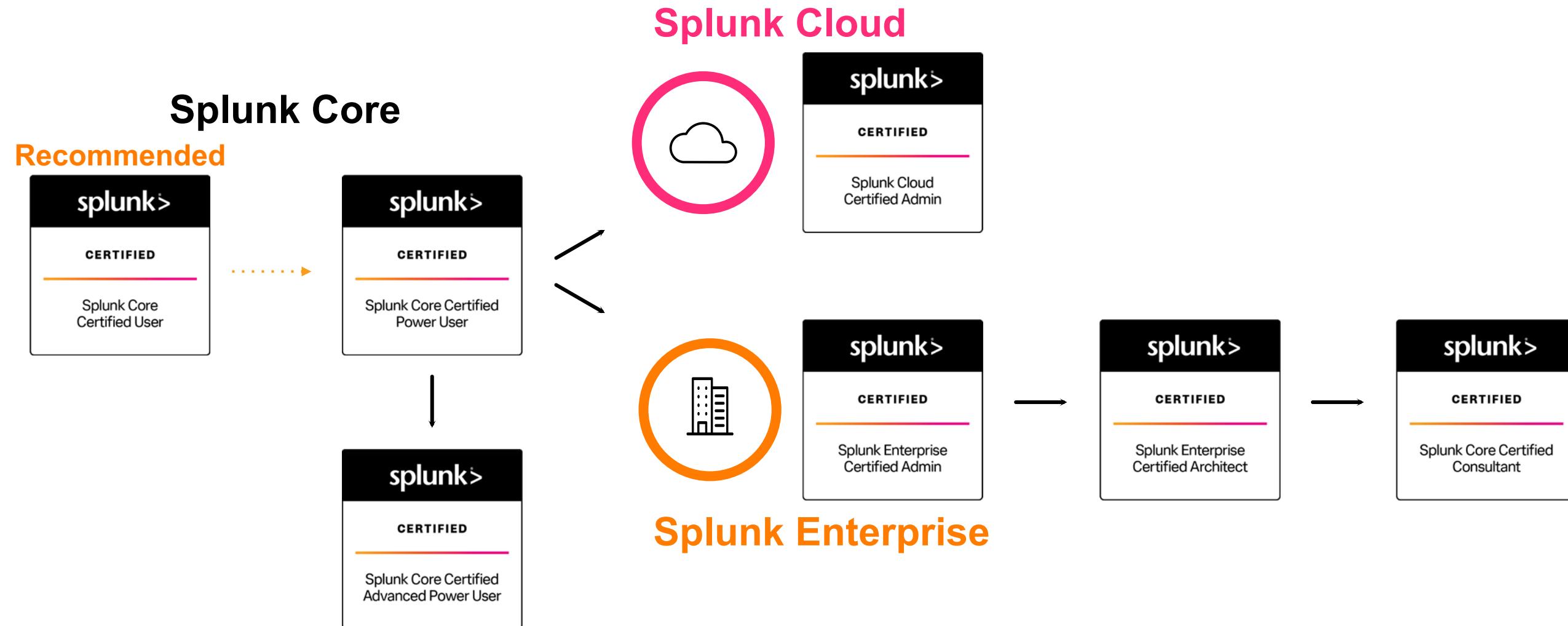
- What is Splunk \*
- Introduction to Splunk \*
- Using Fields \*
- Scheduling Reports and Alerts
- Visualizations
- Statistical Processing
- Working with Time
- Comparing Values
- Result Modification
- Leveraging Lookups and Subsearches
- Correlation Analysis
- Search Under the Hood
- Multivalue Fields
- Search Optimization \*

# Splunk Certification

## Offerings & Requirements

# Splunk Core and Beyond

Regardless of which Splunk product you use, it all starts with Splunk Core



# Splunk Core Certified Power User

This entry-level certification demonstrates an individual's foundational competence of Splunk's core software



## Prerequisite Certification(s):

- None

## Prerequisite Course(s):

- None

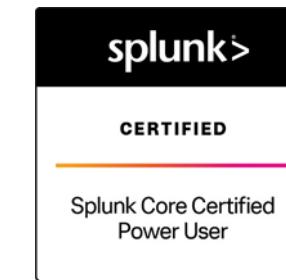
## Splunk Core Certified Power User Exam

Time to [study](#)! We suggest candidates looking to prepare for this exam complete Fundamentals 2 **or** the following courses:

- Visualizations
- Statistical Processing
- Working with Time
- Comparing Values
- Result Modification
- Correlation Analysis
- Search Under the Hood
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Data Models
- Using Choropleth

See [here](#) for registration assistance.

## Congratulations! You are a...



## Recommended Next Steps

- [Splunk Core Certified Advanced Power User](#)
- [Splunk Enterprise Certified Admin](#)
- [Splunk Cloud Certified Admin](#)

# Thank You

---

**splunk**>