Leveraging Lookups and Subsearches

Document Usage Guidelines

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

Copyright © 2023 Splunk, Inc. All rights reserved

Course Goals

- Use lookup commands
- Define subsearch
- Correlate events with subsearches
- Use the **`return`** command in a search

Copyright © 2023 Splunk, Inc. All rights reserved

Course Outline

- Using Lookup Commands
- Adding a Subsearch
- Using the `return` Command

Copyright © 2023 Splunk, Inc. All rights reserved

Using Lookup Commands

Copyright © 2023 Splunk, Inc. All rights reserved

What is a Lookup?

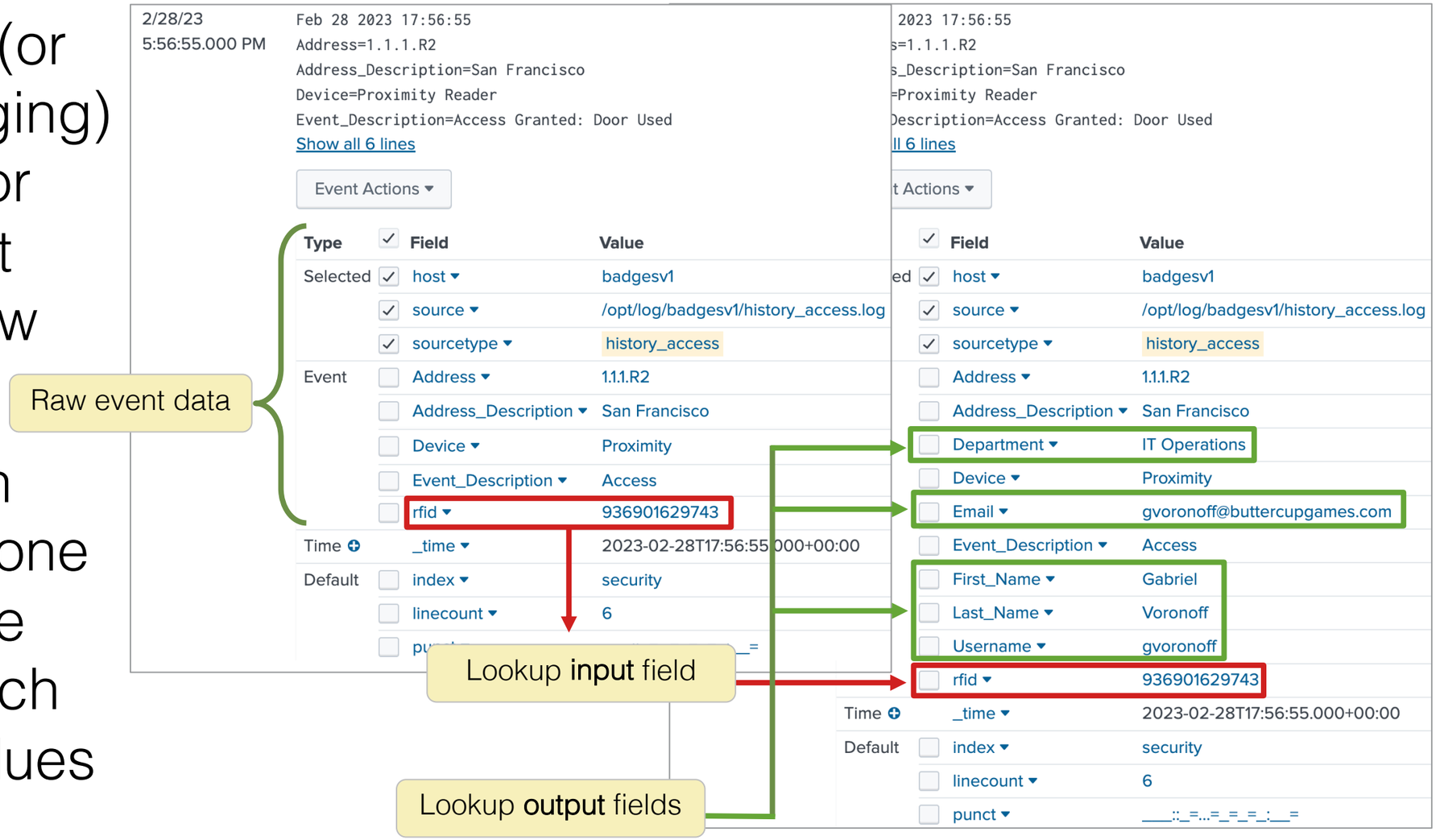
- **Lookups** provide enrichment to your event data by appending fields from another data source (i.e. lookup output fields)
- Splunk provides four types of lookups by default

Lookup Type	Description
File-based	Populates your events with fields pulled from CSV files
External	Uses Python scripts or binary executables to append data
KV Store	Accesses key value pairs from a KV Store collection
Geospatial	References a KMZ or KML file

Copyright © 2023 Splunk, Inc. All rights reserved

Lookups at Search Time

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



Copyright © 2023 Splunk, Inc. All rights reserved

Topic Objectives

- Define lookups
- Use the **`inputlookup`** command to search lookup files
- Use the **`lookup`** command to invoke field value lookups
- Use the **`outputlookup`** command to create lookups
- Use the **`lookup`** command with geospatial lookups

Copyright © 2023 Splunk, Inc. All rights reserved

`inputlookup` Command

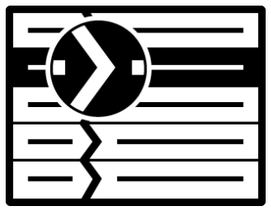
```
| inputlookup [<filename>|<lookup-definition>]
```

- Useful for searching and validating the contents of a lookup table
  - Use **`<filename>`** for searching lookup **`.csv`** or **`.csv.gz`** files
  - Use a lookup's **`<lookup-definition>`** name to search lookup tables configured for any lookup type
- An event-generating command; should be the first command in a search following a pipe character

Copyright © 2023 Splunk, Inc. All rights reserved

`inputlookup` Command Example

Before a lookup can be searched, a knowledge manager must upload the lookup file



`products.csv` lookup file

1. The lookup file is uploaded, and you are given access to the lookup

New Search Save As ▾ Close

2. `| inputlookup products.csv` Last 24 hours ▾

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

Events Patterns **Statistics (14)** Visualization

20 Per Page ▾ Format Preview ▾

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

Copyright © 2023 Splunk, Inc. All rights reserved |

`lookup` Command: Basic Syntax

```
...| lookup <lookup-table-name> <lookup-field>
```

- Use the **`lookup`** command to invoke field value lookups
- The **`<lookup-table-name>`** can reference:
  - Name of CSV file
  - Lookup definition name associated with lookup table files
- The lookup's **`<lookup-field>`** is used to match against the events
- By default, Splunk adds all remaining fields in the lookup table to the events

Copyright © 2023 Splunk, Inc. All rights reserved

lookup Command: <lookup-destfield>

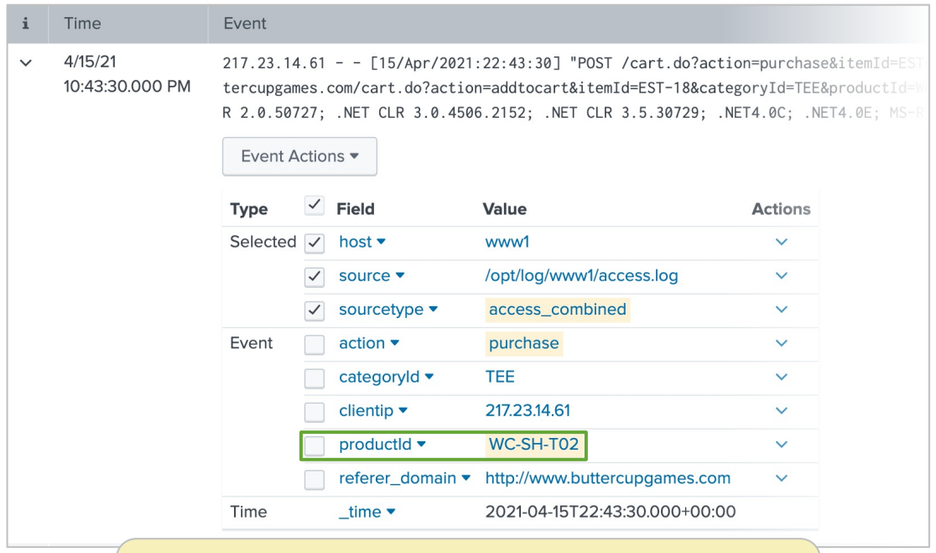
```
...| lookup <lookup-table-name> <lookup-field> [OUTPUT|OUTPUTNEW (<lookup-destfield>)]
```

- You can specify one or more **<lookup-destfield>** to be added to the events; also called "lookup output fields"
- Use modifiers to change overwrite behavior for existing field names that match the lookup output field(s) name(s):
  - **OUTPUT**: overwrite existing fields
  - **OUTPUTNEW**: do not overwrite existing fields
- Lookup output fields only exist for the duration of the search

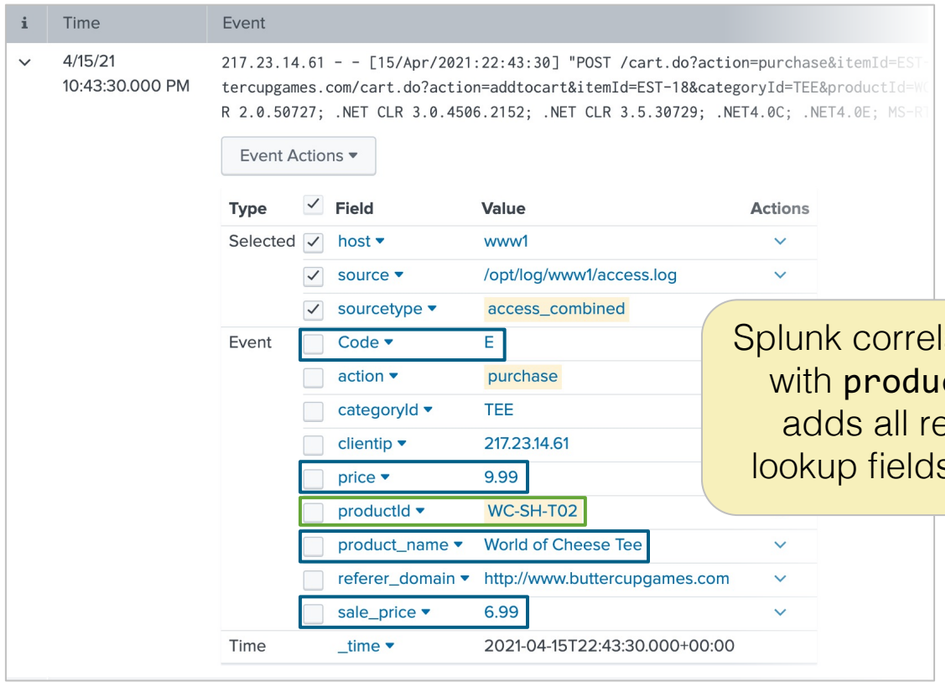
Copyright © 2023 Splunk, Inc. All rights reserved

Enriching Search Results with **Lookup**

- This search invokes **`products.csv`** lookup and Splunk adds additional fields to the search results
- A knowledge manager can configure the searches to always include these fields by making **`products.csv`** an automatic lookup



Event fields before invoking
`| lookup products.csv productId`



Splunk correlates events with **`productId`** and adds all remaining lookup fields to events

Copyright © 2023 Splunk, Inc. All rights reserved

lookup Command Example 1

Scenario

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

```
index=web sourcetype=access* action=purchase status=200
1 | lookup products.csv productId 2 OUTPUT price product_name
3 | stats sum(price) AS sales BY product_name
```

1. Invoke the **products.csv** lookup and use **productId** as the lookup input field
2. Specify price and **product_name** as lookup output fields
3. Lookup output fields are available for statistical processing by **stats**

product_name	sales
Benign Space Debris	2623.95
Curling 2014	1259.37
Dream Crusher	5758.56
Final Sequel	3048.78
Fire Resistance Suit of Provolone	538.65
Holy Blade of Gouda	664.89
Manganiello Bros.	4518.87
Manganiello Bros. Tee	1358.64
Mediocre Kingdoms	3923.43
Orvil the Wolverine	5198.70
Puppies vs. Zombies	513.97
SIM Cubicle	3058.47

Copyright © 2023 Splunk, Inc. All rights reserved |

`lookup` Command Example 2

Scenario

Your Knowledge Manager has just uploaded a new lookup definition for the promotional holiday products. Calculate the sales for each product in the last 24 hours using the promotional sale price.

```
index=web sourcetype=access* action=purchase status=200
| lookup holiday_product_promo productId OUTPUT sale_price product_name
| stats sum(sale_price) AS sales BY product_name
```

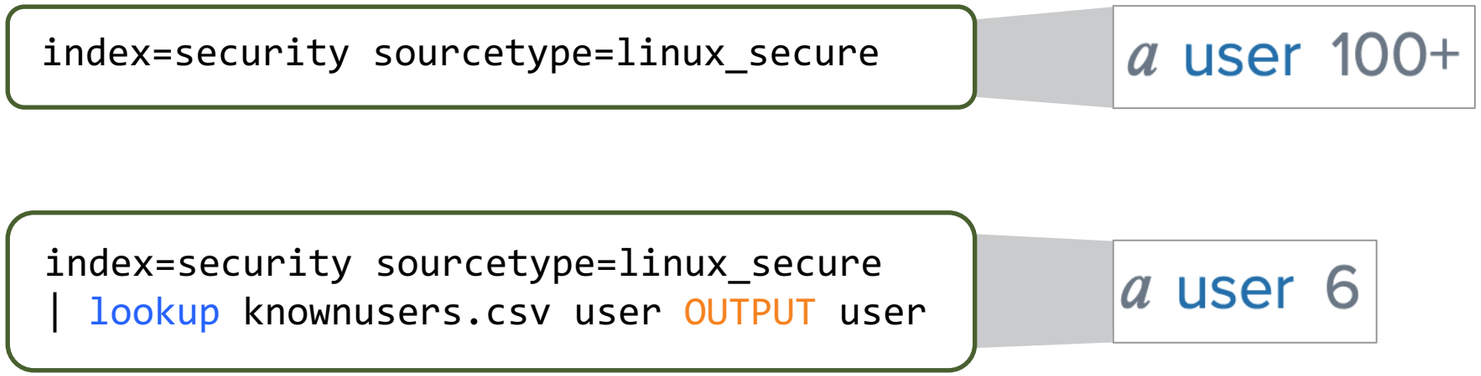
product_name	sales
Curling 2014	1070.37
Dream Crusher	3673.53
Final Sequel	2089.77
SIM Cubicle	2633.45

The lookup definition name is `holiday_product_promo` and the promotional price is `sale_price`

Copyright © 2023 Splunk, Inc. All rights reserved |

Limiting Distinct Values with `lookup`

- Using the same name for **`lookupField`** and **`lookupDestfield`** *can* limit the number of distinct values for **`lookupDestfield`**
- If the value of an event's **`lookupDestfield`** is not present in the values of **`lookupField`** then the value will be set to NULL



Copyright © 2023 Splunk, Inc. All rights reserved

`outputlookup` Command

```
...| outputlookup <filename>|<lookup-definition>
```

- Writes search results to a specified file-based lookup (CSV) or KV Store collection
- Can be executed from a search, ad-hoc report, scheduled search or alert

`users.csv` = filename

```
...|outputlookup users.csv
```

`usergroup` = definition/tablename

```
...|outputlookup usergroup
```

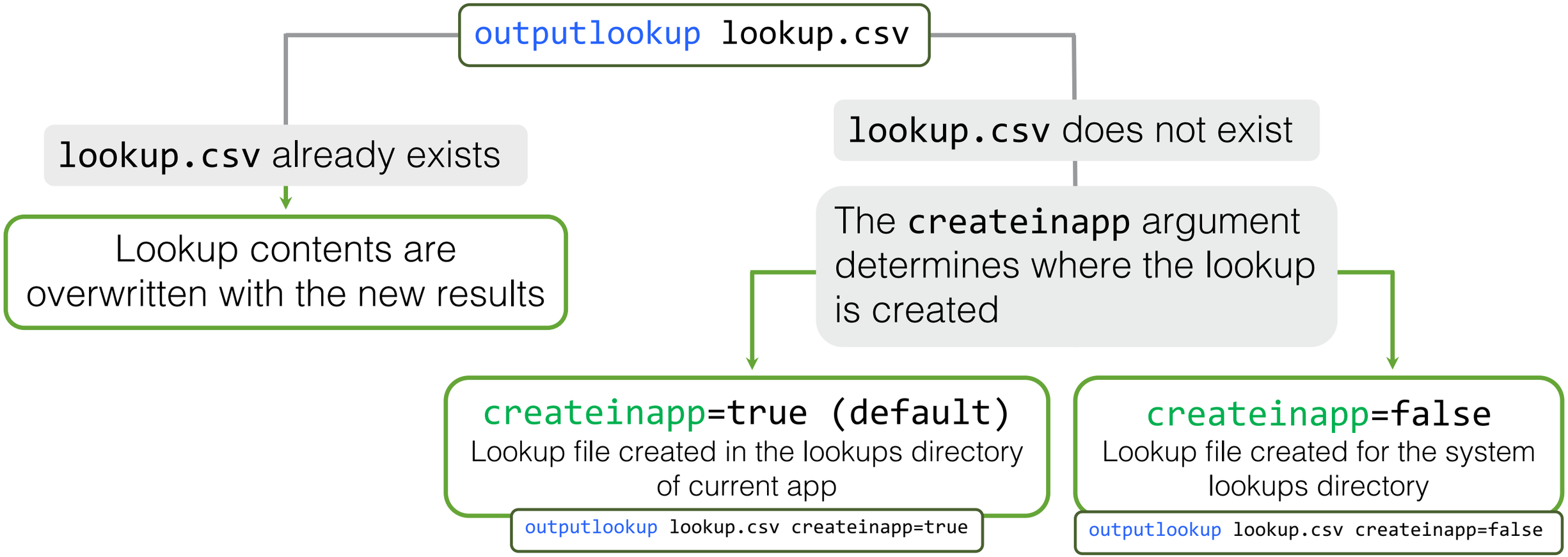
Note

If saving to a lookup definition, the lookup table file or KV collection must already exist.

Copyright © 2023 Splunk, Inc. All rights reserved

`outputlookup` Command (cont.)

The `createinapp` argument is one of many optional arguments

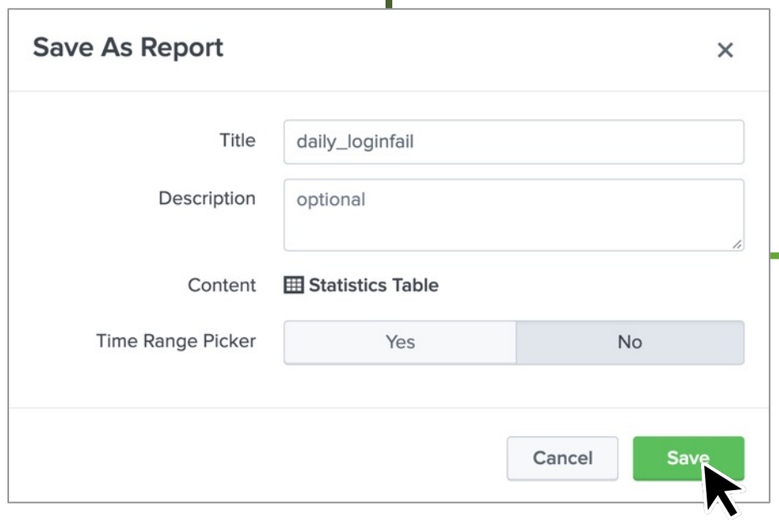


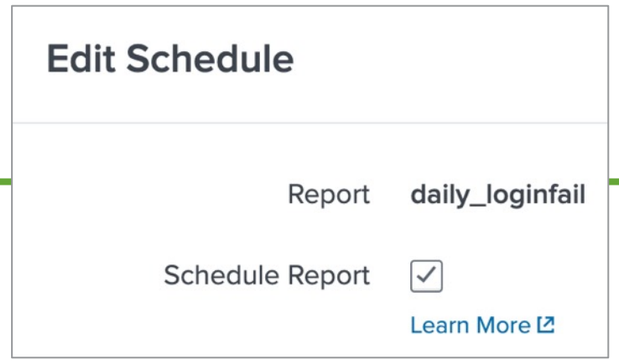
Copyright © 2023 Splunk, Inc. All rights reserved

Using `outputlookup` with Reports

Create an automatically updated lookup with scheduled reports

```
index=security sourcetype=linux_secure "failed password"  earliest=-30d
| stats count by user
| eval daily_average = round(count/30)
| fields - count
| outputlookup averages.csv createinapp=true
```





user	daily_average
abc	16
adm	15
admin	197
administrator	210
agushto	16
alex	16
amanda	15
amavis	16
angel	17
apache	

```
| inputlookup averages.csv
```


Copyright © 2023 Splunk, Inc. All rights reserved

Geospatial Lookups

- Matches region names in your events to region names in lookup and outputs fields with corresponding geographic feature info
- Location coordinate ranges are provided by geographic feature collections: `.KML` and `.KMZ` files
- Geospatial lookups can be invoked in searches to generate choropleth map visualizations
- Splunk ships with two geospatial lookup files:
  - `geo_us_states`
  - `geo_countries`

Copyright © 2023 Splunk, Inc. All rights reserved

Geospatial Lookup Files

- Provides geographic feature information used to define a geospatial lookup
  - **KML**: a type of XML file
  - **KMZ**: a zipped KML file
- Rely on polygons which are closed shapes that start and end at the same coordinate
- Many are available online or can be created from scratch using software such as Google Earth

geo_countries.kml

```
<?xml version="1.0" encoding="utf-8" ?>
<kml xmlns="http://www.opengis.net/kml/2.2">
<Document id="root_doc">
<Schema name="countries" id="countries">
         <SimpleField name="Name" type="string"></SimpleField>
         <SimpleField name="ISO2" type="string"></SimpleField>
         <SimpleField name="ISO3" type="string"></SimpleField>
         <SimpleField name="REGION_WB" type="string"></SimpleField>
         <SimpleField name="REGION_UN" type="string"></SimpleField>
         <SimpleField name="SUBREGION" type="string"></SimpleField>
         <SimpleField name="CONTINENT" type="string"></SimpleField>
</Schema>
<Folder><name>countries</name>
  <Placemark>
         <name>Aruba</name>
         <Style><LineStyle><color>ff0000ff</color></LineStyle><PolyStyle><fill>0</fill></
PolyStyle></Style>
         <ExtendedData><SchemaData schemaUrl="#countries">
                  <SimpleData name="ISO2">AW</SimpleData>
                  <SimpleData name="ISO3">ABW</SimpleData>
                  <SimpleData name="REGION_WB">Latin America &amp; Caribbean</SimpleData>
                  <SimpleData name="REGION_UN">Americas</SimpleData>
                  <SimpleData name="SUBREGION">Caribbean</SimpleData>
                  <SimpleData name="CONTINENT">North America</SimpleData>
         </SchemaData></ExtendedData>
      <Polygon><outerBoundaryIs><LinearRing><coordinates>-
69.996937628999916,12.577582098000036 -69.924672003999945,12.519232489000046 -
69.880197719999842,12.453558661000045 -69.888091600999928,12.417669989000046 -
69.930531378999888,12.425970770000035 -69.945139126999919,12.44037506700009 -
69.924672003999945,12.447211005000014 -70.058094855999883,12.537176825000088 -
70.048736131999931,12.583726304000024 -70.061105923999975,12.625392971000068 -
70.048736131999931,12.632147528000104 -
69.996937628999916,12.577582098000036</coordinates></LinearRing></outerBoundaryIs></
Polygon>
  </Placemark>
```

`geo_countries` content for the island country of Aruba. The `Polygon` tag (highlighted) contains the coordinates Splunk uses to define its choropleth map data.

Copyright © 2023 Splunk, Inc. All rights reserved |

Using Geospatial Lookups: Scenario 1

```
2 index=<index> sourcetype=<sourcetype>
3 | stats count by featureId
4 | geom <geo_lookup>
```

1. Upload and define the KML/KMZ file to Splunk (in this example, the lookup is **`geo_lookup`**)
2. Indicate the events data source that contains either a **`featureId`** or location name field (or **`latitude`** and **`longitude`**; see next slide)
3. Use a transforming command to aggregate data based on the lookup's geographic output field
4. If visualizing results, select and configure a visualization and use the **`geom`** command to generate a choropleth map

Copyright © 2023 Splunk, Inc. All rights reserved

Using Geospatial Lookups: Scenario 2

If the event data source does not contain a **`featureId`** or location name field but does contain values for longitude and latitude, then a lookup must be added with the lookup table name, **`longitude`**, and **`latitude`** as arguments

```
index=<index> sourcetype=<sourcetype>
| lookup geo_lookup latitude longitude
| stats count by featureId
| geom <geo_lookup>
```


Copyright © 2023 Splunk, Inc. All rights reserved

Using Lookup Command Lab Exercise

Time: 30 minutes

Tasks:

- Verify that a lookup has been uploaded correctly
- Use the **`lookup`** command to invoke a lookup in search
- Invoke two lookups in search to find users who have accessed uncategorized URLs over the last 24 hours
- Generate a choropleth map with the **`geom`** command
- Troubleshoot a search that uses the **`lookup`** command
- Challenge: Filter a search by excluding values from a lookup

Copyright © 2023 Splunk, Inc. All rights reserved

Adding a Subsearch

Copyright © 2023 Splunk, Inc. All rights reserved

Topic Objectives

- Define subsearch
- Use subsearch to filter results
- Identify when to use subsearch
- Understand subsearch limitations and alternatives

Copyright © 2023 Splunk, Inc. All rights reserved

What is a Subsearch?

1. When present in a search pipeline, a subsearch is executed first and sends its results to the basic (outer) search
   - Must start with a generating command (**`inputlookup`**, **`search`**, etc.)
   - Enclosed in square brackets
2. Subsearch results are combined with an **`OR`** Boolean and attached to the outer search with an **`AND`** Boolean

```
index=indexName sourcetype=sourcetypeName
  [subsearch] 1
| additional commands
```

1 `[subsearch]` → `field="value1" OR field="value2" OR field="value3"…`

2
```
index=indexName sourcetype=sourcetypeName AND (field="value1"
  OR field="value2" OR field="value3"…)
| additional commands
```

Events from this index/sourcetype containing one of these fields are then processed by the remaining commands in the outer search

Note

Subsearches can return field pairs in the form of
`(field1="valueA" AND field2="valueA") OR`
`(field1="valueB" AND field2="valueB") AND…`

Copyright © 2023 Splunk, Inc. All rights reserved

What is a Subsearch? (cont.)

- Multiple subsearches can be used in a search
- Subsearches can be nested
- Great for filtering data that you cannot describe directly in a search expression

Scenario

Find the most active user over the last 7 days and count this user's events by usage.

```
index=network sourcetype=cisco_wsa_squid
  [search index=network sourcetype=cisco_wsa_squid
   | stats count by username
   | sort -count
   | return 1 username]
| stats count by usage, username
| stats list(usage) as usage,
  list(count) as count by username
```

What the subsearch sends to the outer search

```
username="podessa"
```

username	usage	count
podessa	Borderline	1
	Business	24
	Personal	80
	Unknown	12
	Violation	1

Copyright © 2023 Splunk, Inc. All rights reserved |

Using Subsearch with `inputlookup`

Use a subsearch to access lookup data with `inputlookup` and pass values to the search

```
index=security sourcetype=linux_secure fail* [inputlookup knownusers.csv]
| stats values(src_ip) as attackerIP,
  count as failures by user
| search failures > 3
```

user	attackerIP	failures
djohnson	8.138.86.37	11
myuan	156.235.13.184	12
nsharpe	121.78.152.220 13.180.46.110	110
root	187.231.45.62 188.143.232.202 195.80.144.22 212.235.92.150 24.185.15.226 70.38.1.235	6

user
root
mail
apache
acurry
adombrowski
apreusig
apucci
arangel
basselin
bgenin
bhussain
blu
bsimmel
cberztiss
cfarrell
cganttchart

Excerpt from `knownusers.csv`

Copyright © 2023 Splunk, Inc. All rights reserved

Using Subsearch with `inputlookup` (cont.)

Include a `NOT` operator before a lookup subsearch to exclude lookup values

Scenario

SecOps is finding an increase in penetration attempts. Find unknown users with more than 3 failed logins within the last 60 minutes.

```
index=security sourcetype=linux_secure fail* NOT [inputlookup knownusers.csv]
| stats values(src_ip) as attackerIP,
  count as failures by user
| search failures > 3
| sort -failures
```

user	attackerIP	failures
operator	174.123.217.162 175.44.1.172 194.215.205.19 211.140.3.183 211.191.168.25 27.175.11.11 70.38.1.235 88.191.145.142	9
jira	147.213.138.201 208.240.243.170 211.245.24.3 217.15.20.146 24.185.15.226 89.106.20.218 90.205.111.169 99.61.68.230	8

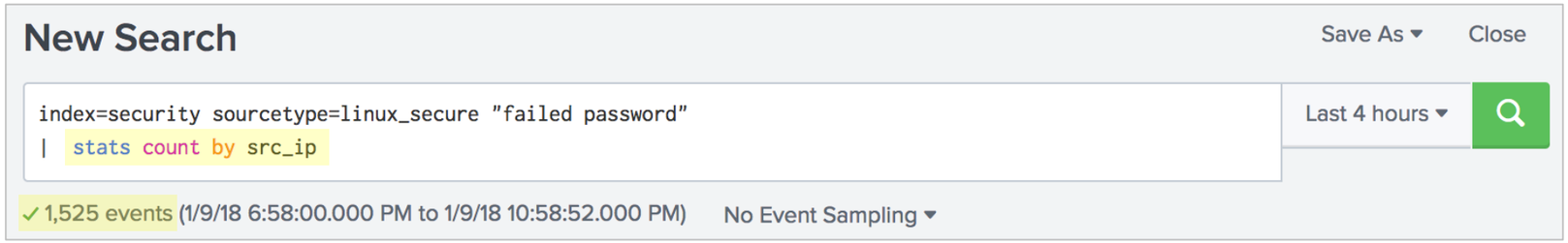
Copyright © 2023 Splunk, Inc. All rights reserved | 1 March 2023

Filtering Through Many Results

- Most hacking attempts begin with many failures from one or more source IP addresses

Scenario

The Security Operations manager wants a list of all IP addresses that might have been used by people trying to hack into the network during the last 4 hours.



- This search counts failures by **`src_ip`** and produces many results
- Let's improve the results and make them more meaningful

Copyright © 2023 Splunk, Inc. All rights reserved

Filtering Through Many Results (cont.)

Scenario

The Security Operations manager wants a list of all IP addresses that might have been used by people trying to hack into the network during the last 4 hours.

```
index=security sourcetype=linux_secure
 "failed password" src_ip!=10.* 1
2| stats count by src_ip
3| where count > 10
```

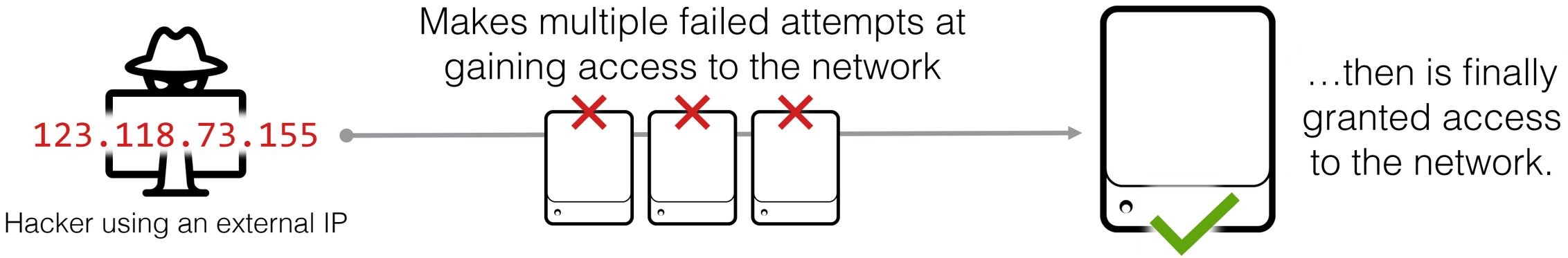
src_ip	count
109.169.32.135	14
123.118.73.155	11
125.89.78.6	12
128.241.220.82	18
133.254.195.96	108
165.238.109.136	109

1. Focus search on failed password attempts from external **src_ip**
2. Count events by **src_ip**
3. Display **src_ip**s with more than 10 associated events

- However, it is still unclear if these **src_ip**s gained network access

Copyright © 2023 Splunk, Inc. All rights reserved |

What are We Trying to Find?



- The external IPs we want to find should be associated with multiple failed attempts and at least one successful attempt
- Use a subsearch to find IPs with multiple failed events
- Then, send these IPs to the outer search to see which IPs eventually gained access to the network

Copyright © 2023 Splunk, Inc. All rights reserved

Filtering with Subsearch

```
index=security sourcetype=linux_secure "accepted"
  [search index=security sourcetype=linux_secure
  "failed password" src_ip!=10.*
  | stats count by src_ip
  | where count > 10
  | fields src_ip]
| dedup src_ip
| table src_ip
```

src_ip
21.116.186.136
52.175.19.220
144.251.73.1
63.239.32.178
67.39.247.107
143.139.165.91

Subsearch

```
[search index=security sourcetype=linux_secure
"failed password" src_ip!=10.*
  | stats count by src_ip
  | where count > 10
  | fields src_ip]
```

```
( ( src_ip="109.169.32.135" ) OR ( src_ip="128.241.220.82" ) OR ( src_ip="141.146.8.66" ) OR ( src_ip="143.139.165.91" )
OR ( src_ip="144.251.73.1" ) OR ( src_ip="188.138.40.166" ) OR ( src_ip="194.215.205.19" ) OR ( src_ip="21.116.186.136" )
OR ( src_ip="211.166.11.101" ) OR ( src_ip="52.175.19.220" ) OR ( src_ip="59.36.99.70" ) OR ( src_ip="63.239.32.178" ) OR
( src_ip="67.39.247.107" ) OR ( src_ip="69.175.97.11" ) OR ( src_ip="82.15.30.214" ) OR ( src_ip="87.194.216.51" ) )
```

Outer search

```
index=security sourcetype=linux_secure "accepted"
AND ( ( src_ip="109.169.32.135" ) OR ( src_ip="128.241.220.82"
) OR ( src_ip="141.146.8.66" ) OR ( src_ip="143.139.165.91" )
OR ( src_ip="144.251.73.1" ) OR ( src_ip="188.138.40.166" ) OR
( src_ip="194.215.205.19" ) OR ( src_ip="21.116.186.136" ) OR (
src_ip="211.166.11.101" ) OR ( src_ip="52.175.19.220" ) OR (
src_ip="59.36.99.70" ) OR ( src_ip="63.239.32.178" ) OR (
src_ip="67.39.247.107" ) OR ( src_ip="69.175.97.11" ) OR (
src_ip="82.15.30.214" ) OR ( src_ip="87.194.216.51" ) )
| dedup src_ip
| table src_ip
```


Copyright © 2023 Splunk, Inc. All rights reserved

Viewing Results of Subsearch with `format`

- Run a subsearch separately with the **`format`** command as the last pipe to view output
- Very useful for troubleshooting subsearches

```
index=security sourcetype=linux_secure "failed password" src_ip!=10.*
| stats count by src_ip
| where count > 10
| fields src_ip
| format
```

```
( ( src_ip="109.169.32.135" ) OR ( src_ip="128.241.220.82" ) OR ( src_ip="141.146.8.66" ) OR ( src_ip="143.139.165.91" )
OR ( src_ip="144.251.73.1" ) OR ( src_ip="188.138.40.166" ) OR ( src_ip="194.215.205.19" ) OR ( src_ip="21.116.186.136" )
OR ( src_ip="211.166.11.101" ) OR ( src_ip="52.175.19.220" ) OR ( src_ip="59.36.99.70" ) OR ( src_ip="63.239.32.178" ) OR
( src_ip="67.39.247.107" ) OR ( src_ip="69.175.97.11" ) OR ( src_ip="82.15.30.214" ) OR ( src_ip="87.194.216.51" ) )
```


Copyright © 2023 Splunk, Inc. All rights reserved

Subsearch Caveats

Subsearches are limited by both time and event count

Default time limit = 60 seconds

- If the subsearch continues to run after this time, it is finalized
- Only the events found during that time are returned to the outer search

Default results limit = 10,000

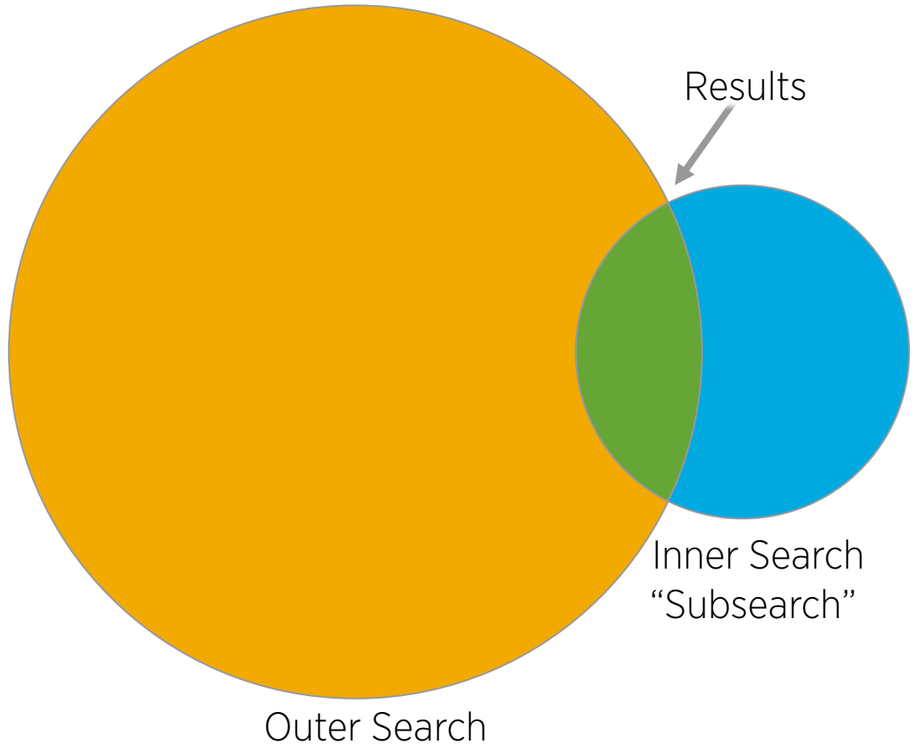
- When the limit is met, the results are truncated (partial result set)

- If the outer search executes in real-time, the subsearch executes over all time by default
  - Executing over all time is not recommended for subsearches
  - Use `earliest` and `latest` in subsearch to avoid executing over all time

Copyright © 2023 Splunk, Inc. All rights reserved

When to Use Subsearch

Subsearch passes results to the outer search for filtering; therefore, subsearches work best if they produce a small result set



Copyright © 2023 Splunk, Inc. All rights reserved

Alternatives to Subsearch

- If a subsearch produces many results, then it is generally more efficient to use **`stats`** and **`eval`**
- Subsearches take longer than other types of searches
- Searches that execute often, e.g. scheduled reports or searches executed from the dashboard, should not use subsearches

Copyright © 2023 Splunk, Inc. All rights reserved

Finding "Tailgaters" with Subsearch

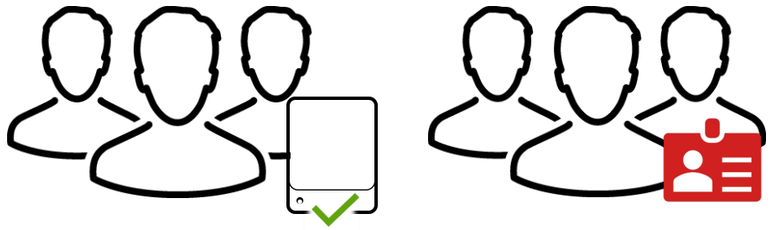
Scenario

The CSO wants a list of tailgaters during the last 4 hours.

A tailgater is someone who logged into the network but did not badge into the building

Create a subsearch to find unique users who badged into the building

Create an outer search to find users who logged into the network but did not appear in subsearch results



Copyright © 2023 Splunk, Inc. All rights reserved | 1 March 2023

Finding "Tailgaters" with Subsearch (cont.)

Scenario

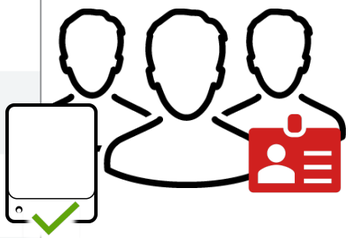
The CSO wants a list of tailgaters during the last 4 hours.

1. Use subsearch to find unique users who badged in
2. Find users who logged onto the network
3. Filter outer search results by excluding users found in the subsearch

```
2 index=security sourcetype=winauthentication_security
(EventCode=540 OR EventCode=4624)
3 NOT
        [search index=security
        sourcetype=history_access
        Event_Description=Access
        | dedup User
        | fields User]
| stats count by User
| fields - count
```

1

User
arangel
dtempesti
svoronoff
tzielinski



Copyright © 2023 Splunk, Inc. All rights reserved

Finding "Tailgaters" with `eval` and `stats`

If you are working with a large set of data, use eval with stats for better search performance

```
(index=security sourcetype=winauthentication_security
(EventCode=540 OR EventCode=4624))
OR (index=security sourcetype=history_access
Event_Description=Access)
| eval badge_access = if(sourcetype="history_access", 1, 0)
| stats max(badge_access) as badged_in by User
| where badged_in = 0
| sort User
| fields - badged_in
```

This search has completed and has returned **72** results by scanning **3,564** events in **0.392** seconds

Using **eval** and **stats** completes 30% faster

This search has completed and has returned **72** results by scanning **1,156** events in **0.575** seconds

Using subsearch

Copyright © 2023 Splunk, Inc. All rights reserved

Troubleshooting Subsearches

- Click after a bracket or parenthesis and a box encloses the corresponding item
- Run both searches independently to confirm events are being returned and to gain an understanding of the data

```
index=security sourcetype=linux_secure
"accepted"
[ search index=security
  sourcetype=linux_secure "failed password"
  src_ip!=10.*
| stats count by src_ip
| where count > 10
| fields src_ip ]
| dedup src_ip
| table src_ip
```

- Know when it's efficient to use subsearch versus using a search with **`eval`** and **`stats`**

Copyright © 2023 Splunk, Inc. All rights reserved

Adding a Subsearch Lab Exercise

Time: 15 minutes

Tasks:

- Use a subsearch and a lookup to filter search results
- Combine two searches to create a single search with an outer search and an inner subsearch

Copyright © 2023 Splunk, Inc. All rights reserved

Using the `return` Command

Copyright © 2023 Splunk, Inc. All rights reserved

Topic Objectives

- Use the **`return`** command
- Compare **`return`** and **`fields`** commands

Copyright © 2023 Splunk, Inc. All rights reserved

`return` Results from a Subsearch

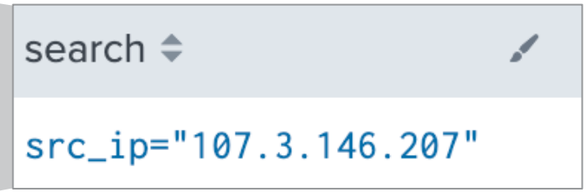
```
...| return [<count>] [<field>…][<alias>=<field>…][$<field>…]
```

- Used to pass values from a subsearch to the outer search
- **`<count>`** is an integer that tells Splunk how many rows of results to return; by default, Splunk only returns the first row
- Specify one or more **`<field>`** to return, separated by spaces
  - Use **`$<field>`** to return just the values (i.e. no field name)
  - Use **`<alias>=<field>`** to return and rename fields

Copyright © 2023 Splunk, Inc. All rights reserved

`return` Command Examples

```
index=security sourcetype=linux_secure
"failed password" src_ip!=10.*
| stats count by src_ip
| where count>10
| return src_ip
```




```
index=security sourcetype=linux_secure
"failed password" src_ip!=10.*
| stats count by src_ip
| where count>10
| return $src_ip
```


```
index=security sourcetype=linux_secure
"failed password" src_ip!=10.*
| stats count by src_ip
| where count>10
| return ip=src_ip
```

Copyright © 2023 Splunk, Inc. All rights reserved

`return` versus `fields`

Send all values to the outer search with **`fields`** or use **`return`** if you want more control over how results are sent to the outer search

Using **`return`** gives you more control over how many values to return and whether to return the field name

```
index=security sourcetype=linux_secure
"failed password" src_ip!=10.*
| stats count by src_ip
| where count>10
| sort -count
| return 3 src_ip
```

search

```
(src_ip="21.116.186.136") OR (src_ip="52.175.19.220") OR (src_ip="67.39.247.107")
```

`fields` sends all key-value pairs for **`src_ip`** that satisfied the search

```
index=security sourcetype=linux_secure
"failed password" src_ip!=10.*
| stats count by src_ip
| where count>10
| sort -count
| fields src_ip
```

search

```
( ( src_ip="21.116.186.136" ) OR ( src_ip="52.175.19.220" ) OR ( src_ip="67.39.247.107" ) (
( src_ip="82.15.30.214" ) OR ( src_ip="63.239.32.178" ) OR ( src_ip="87.194.216.51" ) OR (
src_ip="109.169.32.135" ) OR ( src_ip="128.241.220.82" ) OR ( src_ip="188.138.40.166" ) OR
( src_ip="216.221.226.11" ) )
```


Copyright © 2023 Splunk, Inc. All rights reserved

Using the `return` Command Lab Exercise

Time: 10 minutes

Tasks:

- Return search results as key-value pairs
- Use a subsearch to return key-value pairs from a lookup and use these values to filter search results

Copyright © 2023 Splunk, Inc. All rights reserved

Wrap-up Slides

Copyright © 2023 Splunk, Inc. All rights reserved

Wrap-up

- You should now be able to:
  - Use **`lookup`**, **`inputlookup`** commands and subsearches to enrich and filter search results
  - Use the **`return`** command to control how subsearch results are sent to the main search

Copyright © 2023 Splunk, Inc. All rights reserved

Community

- Splunk Community Portal – community.splunk.com
  - Answers
  - Discussions
  - Splunk Trust
  - User Groups
  - Ideas
- Splunk Blogs – splunk.com/blog/
- Splunk Base – splunkbase.com
  - Apps
  - Curated Collections
- Splunk Docs on Twitter – twitter.com/splunkdocs
- Splunk Dev on Twitter – twitter.com/splunkdev
- Splunk on Slack – splk.it/slack
- .conf – conf.splunk.com

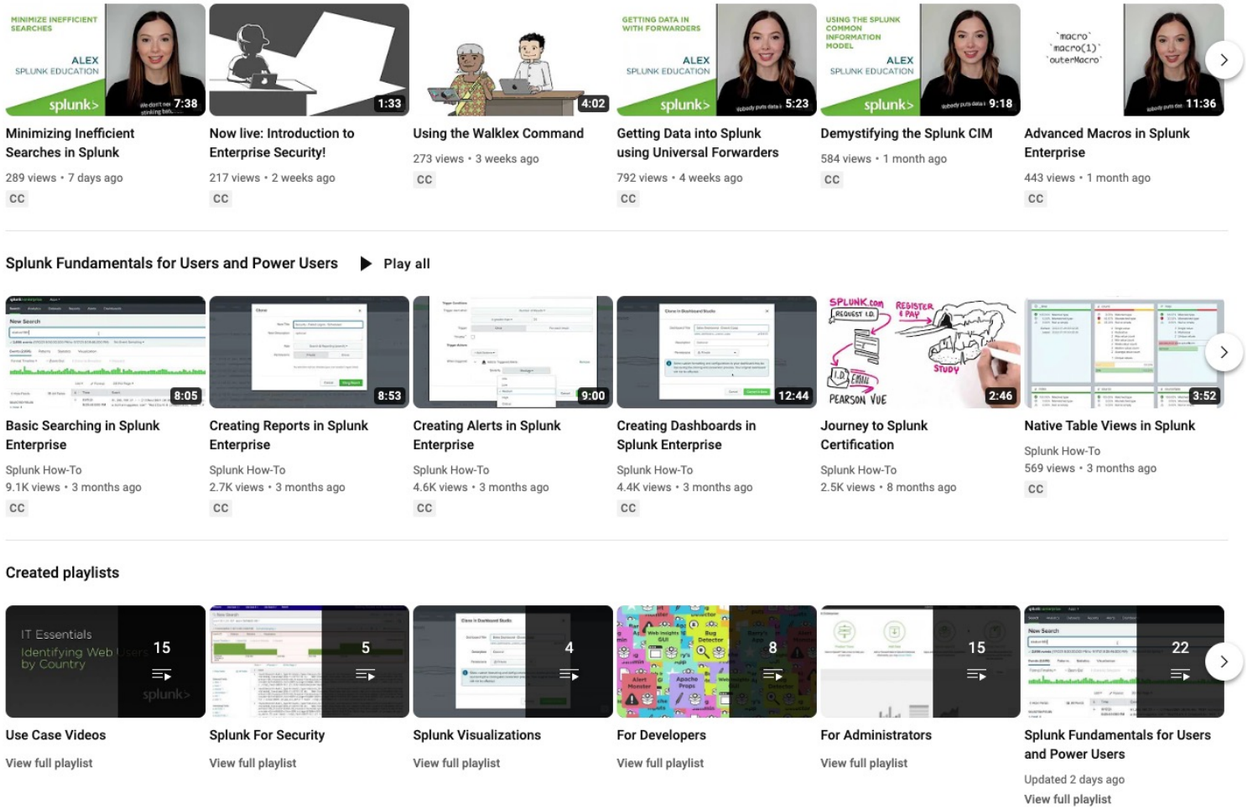
Community

- Knowledge Base – Search knowledge base, answers, and docs to troubleshoot your issue
- splunk>dev – Documentation for developers
- Splunk Docs – Product, best practices, and tools documentation for all Splunk products
- Splunk Lantern – Actionable guidance by experts
- Create a case – Support for critical issues
- Contact Us – Find region-specific support
  - (855) SPLUNK.S or (855) 775.8657
  - Not in the US? Find your local office
- System Status – Cloud Services, Observability Cloud, Splunk On-Call, Synthetic Monitoring
- Splunk Product Security – Critical Security Alerts, Quarterly Security Patches, and 3rd Party Bulletins

© 2022 SPLUNK INC.

Splunk How-To Channel

Free, short videos on a variety of Splunk topics: splk.it/How-To



Copyright © 2023 Splunk, Inc. All rights reserved

Learning Paths

Search Expert – Recommended Courses

Free eLearning courses are highlighted 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 *

Copyright © 2023 Splunk, Inc. All rights reserved

Learning Paths

Knowledge Manager – Recommended Courses

Free eLearning courses are highlighted 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 *

Copyright © 2023 Splunk, Inc. All rights reserved

© 2022 SPLUNK INC.

Splunk Mobile

- Free app available to all Splunk Cloud and Splunk Enterprise customers
- Analyze data and receive actionable alerts on-the-go with mobile-friendly dashboards
- iOS and Android
- See the Product Brief
- Download for iOS splk.it/ios

Copyright © 2023 Splunk, Inc. All rights reserved | 1 March 2023

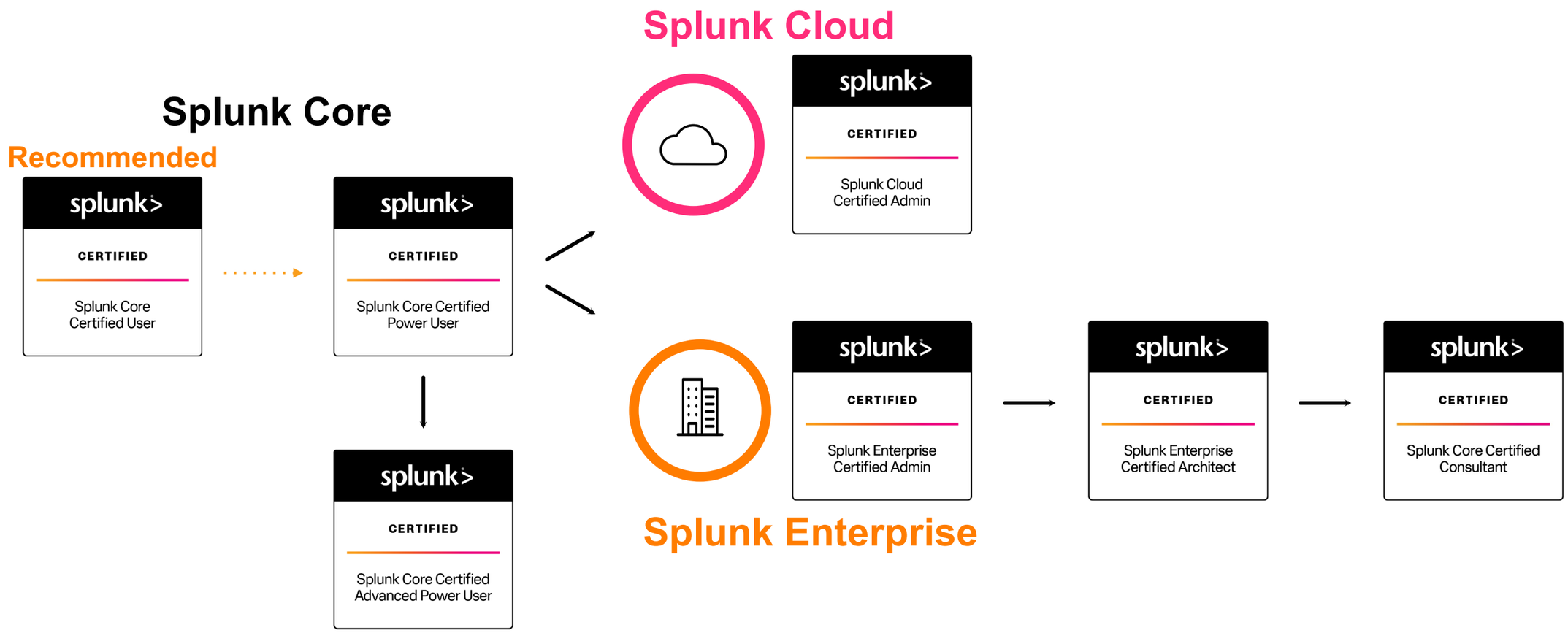
Splunk Certification

Offerings & Requirements

Copyright © 2023 Splunk, Inc. All rights reserved

Splunk Core and Beyond

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



App-Specific Offerings

For Splunk Add-Ons

App Developer

ES Administration

ITSI Administration

SOAR Automation Developer

Splunk Core Certified User

This entry-level certification demonstrates an individual's basic ability to navigate and use Splunk software

Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

Splunk Core Certified User Exam

Time to study! We suggest candidates looking to prepare for this exam complete Fundamentals 1 **or** the following courses:

- What is Splunk?
- Intro to Splunk
- Using Fields
- Scheduling Reports and Alerts
- Visualizations
- Statistical Processing
- Working with Time
- Leveraging Lookups and Subsearches
- Search Optimization
- Enriching Data with Lookups
- Data Models

See here for registration assistance.

Congratulations! You are a...

Recommended Next Step

- Splunk Core Certified Power User

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

Splunk Core Certified Advanced Power User

This certification demonstrates an individual's ability to generate complex searches, reports, and dashboards with Splunk's core software to get the most out of their data

Prerequisite Certification(s):

- Splunk Core Certified Power User

Prerequisite Course(s):

- None

Splunk Core Certified Advanced Power User Exam

Time to study! We suggest candidates looking to prepare for this exam complete Fundamentals 3, Creating Dashboards, and Advanced Searching & Reporting **or** the following courses:

- Using Fields
- Working with Time
- Comparing Values
- Result Modification
- Leveraging Lookups and Subsearches
- Correlation Analysis
- Search Under the Hood
- Multivalue Fields
- Search Optimization
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Using Choropleth
- Introduction to Dashboards
- Dynamic Dashboards

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- Splunk Enterprise Certified Admin
- Splunk Cloud Certified Admin

Splunk Cloud Certified Admin

This certification demonstrates an individual's ability to support the day-to-day administration and health of a Splunk Cloud environment

Prerequisite Certification(s):

- Splunk Core Certified Power User

Prerequisite Course(s):

- None

Splunk Cloud Certified Admin Exam

Time to study! We suggest candidates looking to prepare for this exam complete **either** the Splunk Cloud Administration **or** the Transitioning to Splunk Cloud course.

Both courses will equally prepare candidates for the exam, but are tailored to meet the needs of the individual based on prior Splunk experience.

Splunk Cloud Administration is designed for net-new administrators working in a Splunk Cloud environment. **Transitioning to Splunk Cloud** is for experienced Enterprise administrators looking to maximize their success in migrating to a Cloud environment.

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- Splunk Certified Developer

Splunk Enterprise Certified Admin

This certification demonstrates an individual's ability to support the day-to-day administration and health of a Splunk Enterprise environment

Prerequisite Certification(s):

- Splunk Core Certified Power User

Prerequisite Course(s):

- None

Splunk Enterprise Certified Admin Exam

Time to study! We suggest candidates looking to prepare for this exam complete the following courses:

- Splunk System Administration
- Splunk Data Administration

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- Splunk Enterprise Certified Architect
- Splunk Certified Developer

Splunk Certified Architect

This certification demonstrates an individual's ability to deploy, manage, and troubleshoot complex Splunk Enterprise environments

Prerequisite Certification(s):

- Splunk Core Certified Power User
- Splunk Enterprise Certified Admin

Prerequisite Course(s):

- Architecting Splunk Enterprise Deployments
- Troubleshooting Splunk Enterprise
- Splunk Cluster Administration
- Splunk Deployment Practical Lab

Splunk Enterprise Certified Architect Exam

Time to study! We **require** candidates looking to register for this exam to complete the following prerequisite courses:

- Architecting Splunk Enterprise Deployments
- Troubleshooting Splunk Enterprise
- Splunk Cluster Administration
- Splunk Deployment Practical Lab

Candidates who are **Splunk Enterprise Certified Admin** and have completed all of the above courses will automatically receive an exam authorization for the Splunk Enterprise Certified Architect exam within 5-7 business days of receiving their passing lab results.

See here for registration assistance.

Congratulations! You are a...

splunk>

CERTIFIED

Splunk Enterprise Certified Architect

Recommended Next Steps

- Splunk Core Certified Consultant

Splunk Core Certified Consultant

This certification demonstrates an individual's ability to properly size, install, and implement Splunk environments and to advise others on how to utilize the product and maximize its value for their needs

Prerequisite Certification(s):

- Splunk Core Certified Power User
- Splunk Enterprise Certified Admin
- Splunk Enterprise Certified Architect

Prerequisite Course(s):

- *Advanced Power User courses **or** digital badge**
- Core Consultant Labs
  - Indexer Cluster Implementation
  - Distributed Search Migration
  - Implementation Fundamentals
  - Architect Implementation 1-3
- Services Core Implementation

Splunk Core Certified Consultant Exam

Time to study! We **require** candidates looking to register for this exam to complete the following prerequisite courses:

- *Fundamentals 3*, *Creating Dashboards*, *Advanced Searching & Reporting**
- Core Consultant Labs
- Services Core Implementation

Candidates who are **Splunk Enterprise Certified Architects** and have completed all of the above courses must contact certification@splunk.com to request their Core Consultant exam authorization.

See here for registration assistance.

These Advanced Power User courses can be replaced with a Splunk Certified Advanced Power User badge **or completion of the following courses:*

- Using Fields
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Search Optimization
- Working with Time
- Leveraging Lookups and Subsearches
- Comparing Values
- Correlation Analysis
- Result Modification
- Multivalue Fields
- Search Under the Hood
- Introduction to Dashboards
- Dynamic Dashboards
- Using Choropleth

Congratulations! You are a...

Recommended Next Steps

- None

Splunk Certified Developer

This certification demonstrates an individual's expertise in drilldowns, advanced behaviors and visualizations, planning, creating, and packaging apps, and REST endpoints

Prerequisite Certification(s):

- Splunk Core Certified Power User

AND

- Splunk Enterprise Certified Admin

OR

- Splunk Cloud Certified Admin

Prerequisite Course(s):

- None

Splunk Certified Developer Exam

Time to study! We suggest candidates looking to prepare for this exam complete the following courses:

- Creating Dashboards with Splunk*
- Advanced Dashboards & Visualizations
- Building Splunk Apps
- Developing with Splunk's REST API

This course may also be substituted with the following newly-launched courses:

- Introduction to Dashboards
- Dynamic Dashboards
- Using Choropleth

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- None

Splunk Enterprise Security Certified Admin

This certification demonstrates an individual's ability to install, configure, and manage a Splunk Enterprise Security deployment

Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

Splunk Enterprise Security Certified Admin Exam

Time to study! We suggest candidates looking to prepare for this exam complete the following course:

- Administering Splunk Enterprise Security

Please note: all candidates are expected to have working knowledge and experience as either Splunk Cloud or Splunk Enterprise Administrators.

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- Splunk Phantom Certified Admin

Splunk IT Service Intelligence Certified Admin

This certification demonstrates an individual's ability to deploy, manage, and utilize Splunk ITSI to monitor mission-critical services

Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

Splunk IT Service Intelligence Certified Admin Exam

Time to study! We suggest candidates looking to prepare for this exam complete the following course:

- Implementing Splunk IT Service Intelligence

Please note: all candidates are expected to have working knowledge and experience as either Splunk Cloud or Splunk Enterprise Administrators.

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- Courses on Observability

Splunk SOAR Certified Automation Developer

This certification demonstrates an individual's ability to install and configure a SOAR server, integrate it with Splunk, and plan, design, create, and debug playbooks

Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

Splunk SOAR Certified Automation Developer Exam

Time to study! We suggest candidates looking to prepare for this exam complete the following courses:

- Administering SOAR (Phantom)
- Developing SOAR (Phantom) Playbooks
- Advanced SOAR (Phantom) Implementation

Please note: all candidates are expected to have working knowledge and experience as either Splunk Cloud or Splunk Enterprise Administrators.

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- None

© 2022 SPLUNK INC.

Thank You

splunk> turn data into doing™