Splunk4Rookies - Security

#Splunk4Rookies

Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk>

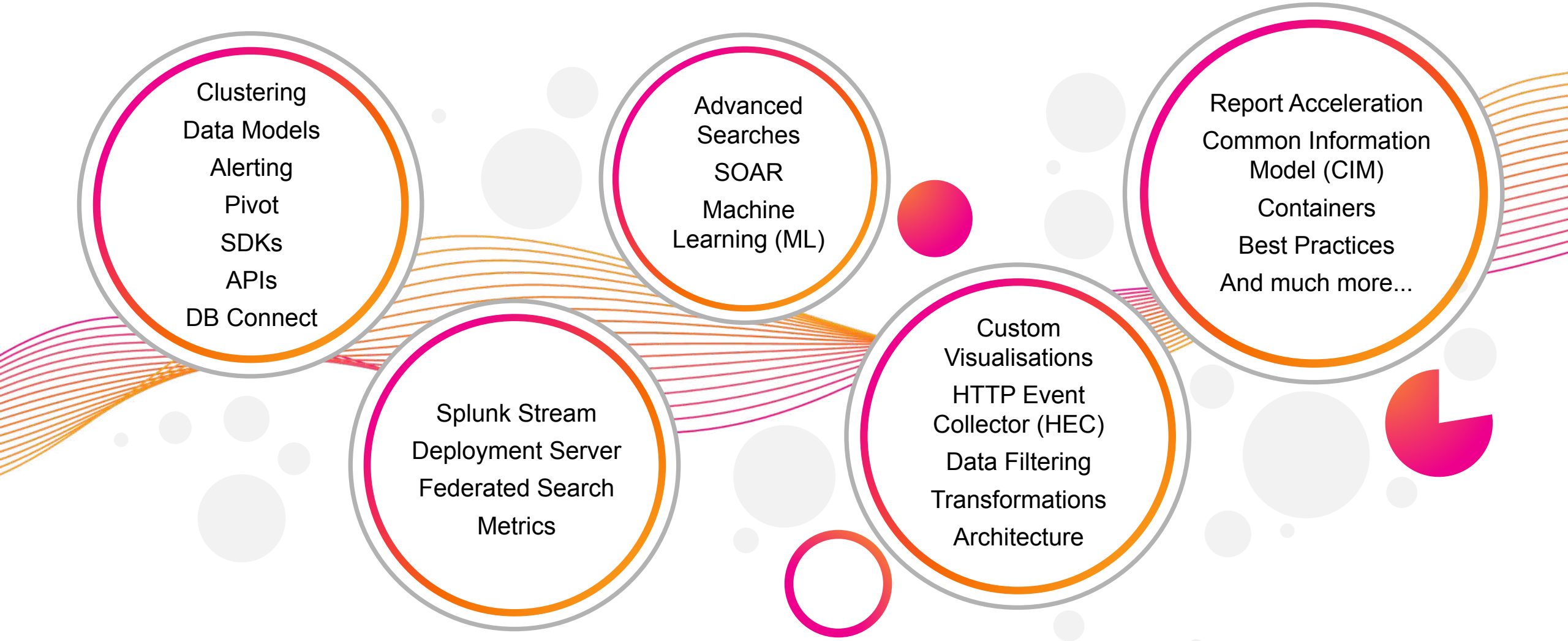
Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?

Workshop Agenda

- Brief Splunk overview
- Search basics
- Indexing data
- Defining the format of your data
- Making data useable
- Aggregating and correlating data
- Put it into practice on web defacement investigation
- Creating proactive searches and dashboards

There's a Lot More to Splunk



Visit https://splunk.com/training to learn more!

splunk>

Objective for Today

splunk>

REGISTRATION 5 MINS

Enroll in Today's Workshop

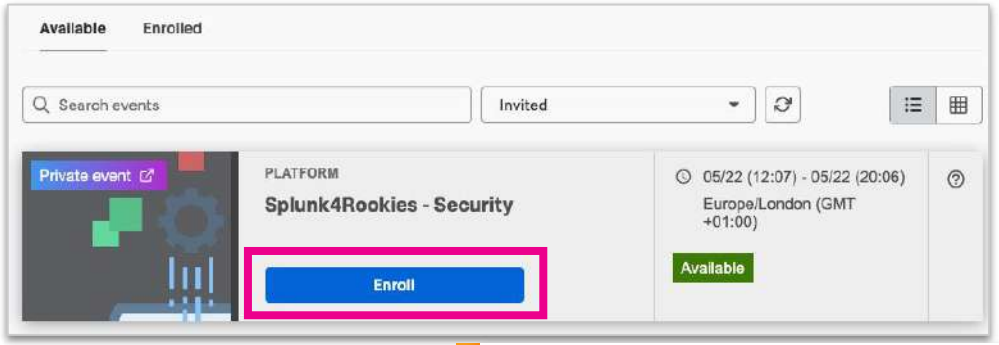
Tasks

1. Get a splunk.com account if you don't have one yet:
   https://splk.it/SignUp

2. Enroll in the Splunk Show workshop event:
   https://show.splunk.com/event/<eventID>

3. Download a copy of today's slide deck:
   https://splk.it/S4RS-Attendee

Goal



Enroll in today's event

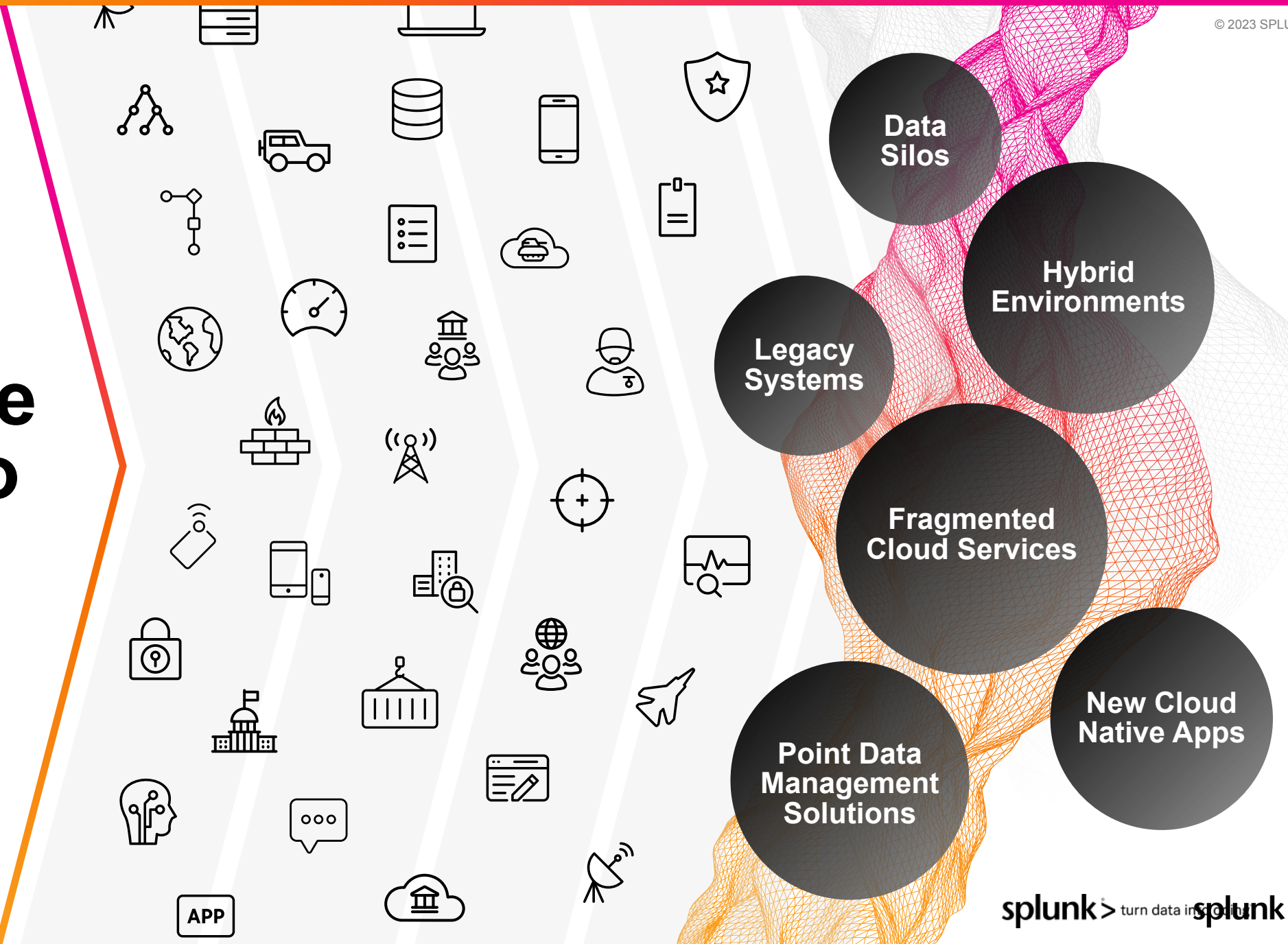
splunk>

Data is your Competitive Advantage

Data isn't just a record.
Data makes things happen.
Splunk makes it possible.

splunk> turn data into doing

Turning Real-time Data Into Action is Hard



The Power of Splunk

Delivering Unified Security and Observability

See

End-to-end visibility

No sampling or blind spots

Act

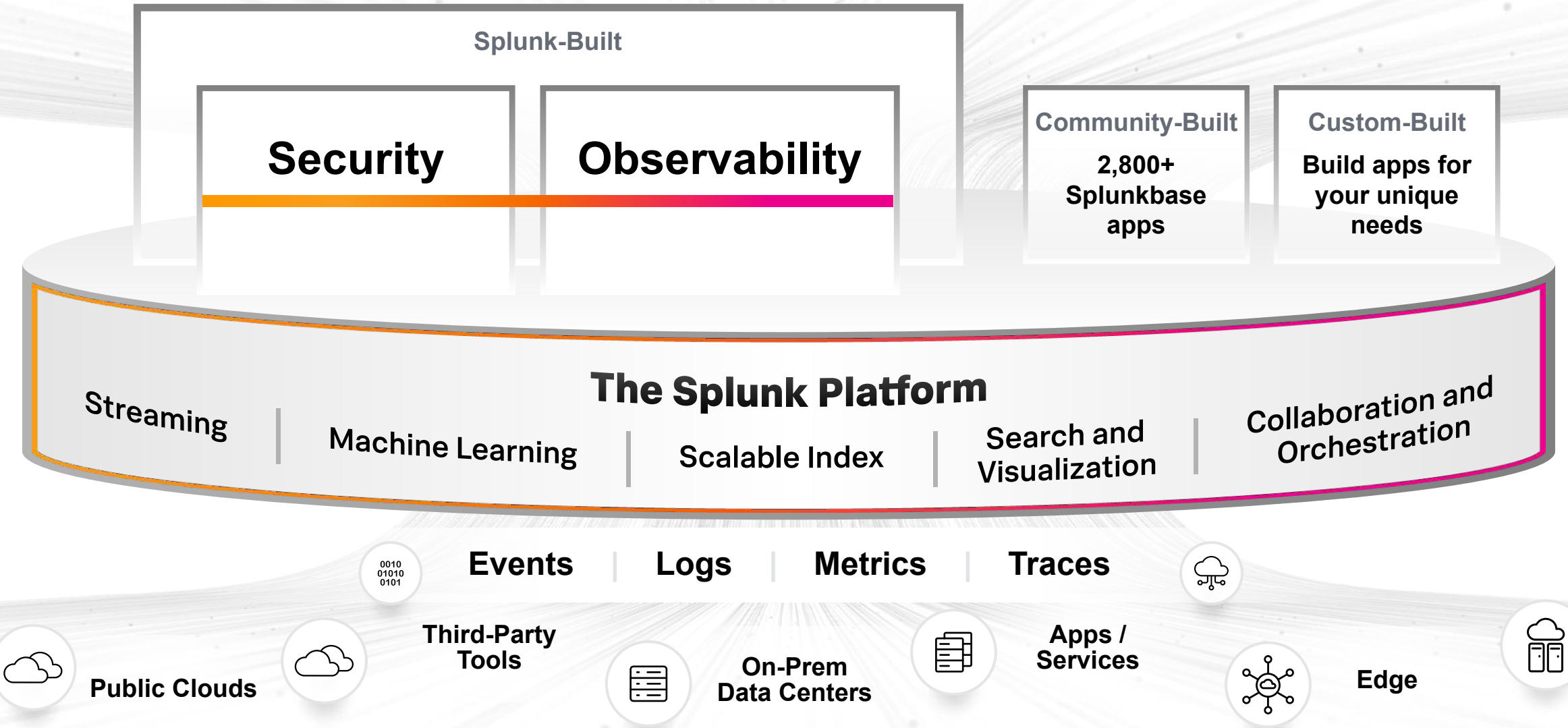
Investigate across massive data sets and take **action** fast

Extend

Extend the **platform** to use data to solve problems across the business

splunk>

The Unified Security and Observability Platform



Splunk as a Service

Fastest time to value | Minimum Infrastructure | Maximum Value

3 Simple Steps

1. Onboard data
2. Onboard users
3. Get value from your data

splunk>cloud™

- **Fastest time to value**
- **Software as a service** - AWS or GCP
- **Secure** - ISO 27001, SOC 2 Type II, PCI, HIPAA, FedRAMP (Moderate)
- **Encryption-in-transit** - plus optional encryption-at-rest
- **Resilient infrastructure**
- **100% uptime guarantee**
- **24/7 NOC/SOC support team**

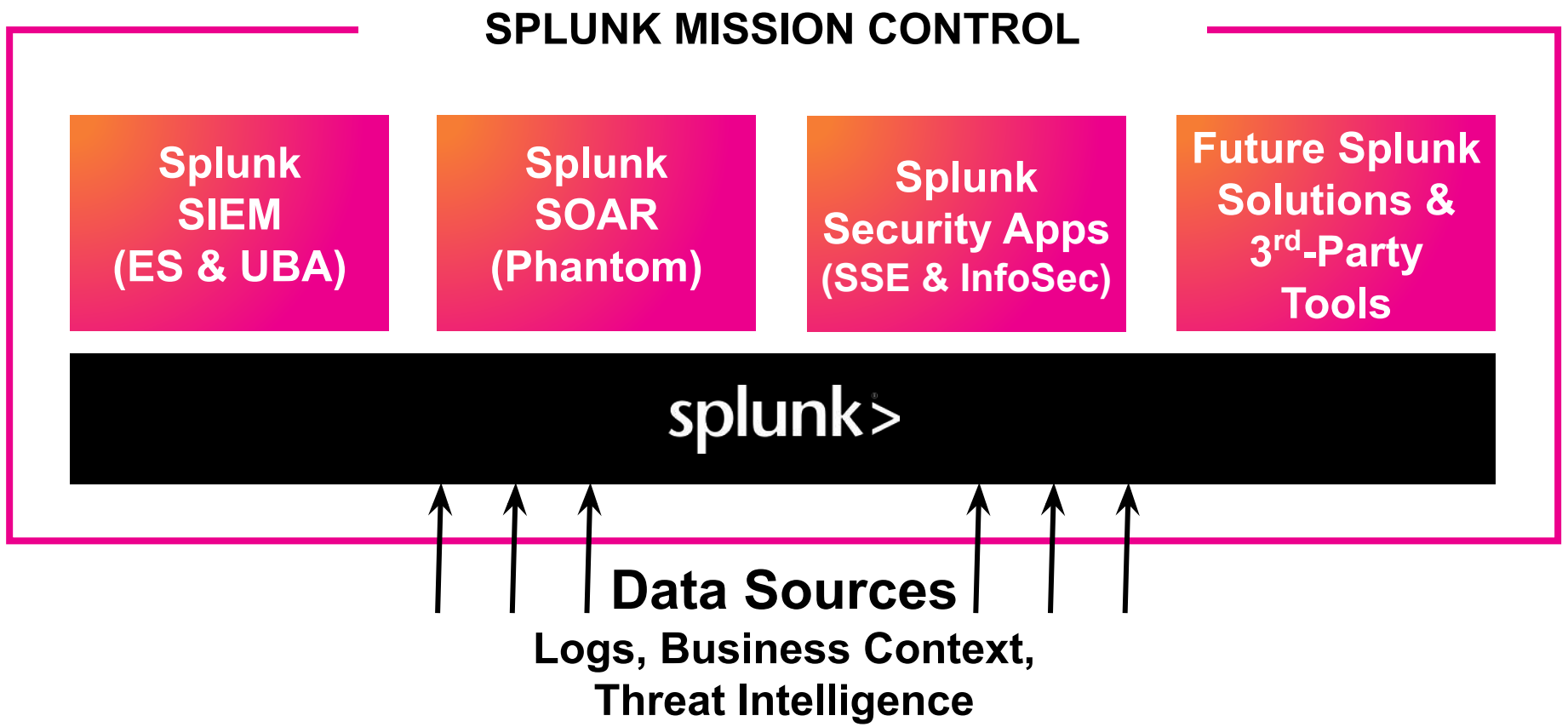
Flexible options for data collection and forwarding

Splunk Cloud Service Description: https://splk.it/SplunkCloudServDesc

splunk>

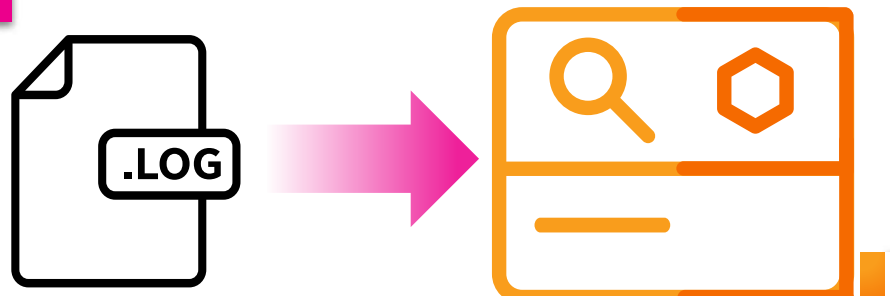
Splunk for Security

Unifying **data**, **analytics**, and **operations**



Today's Environment

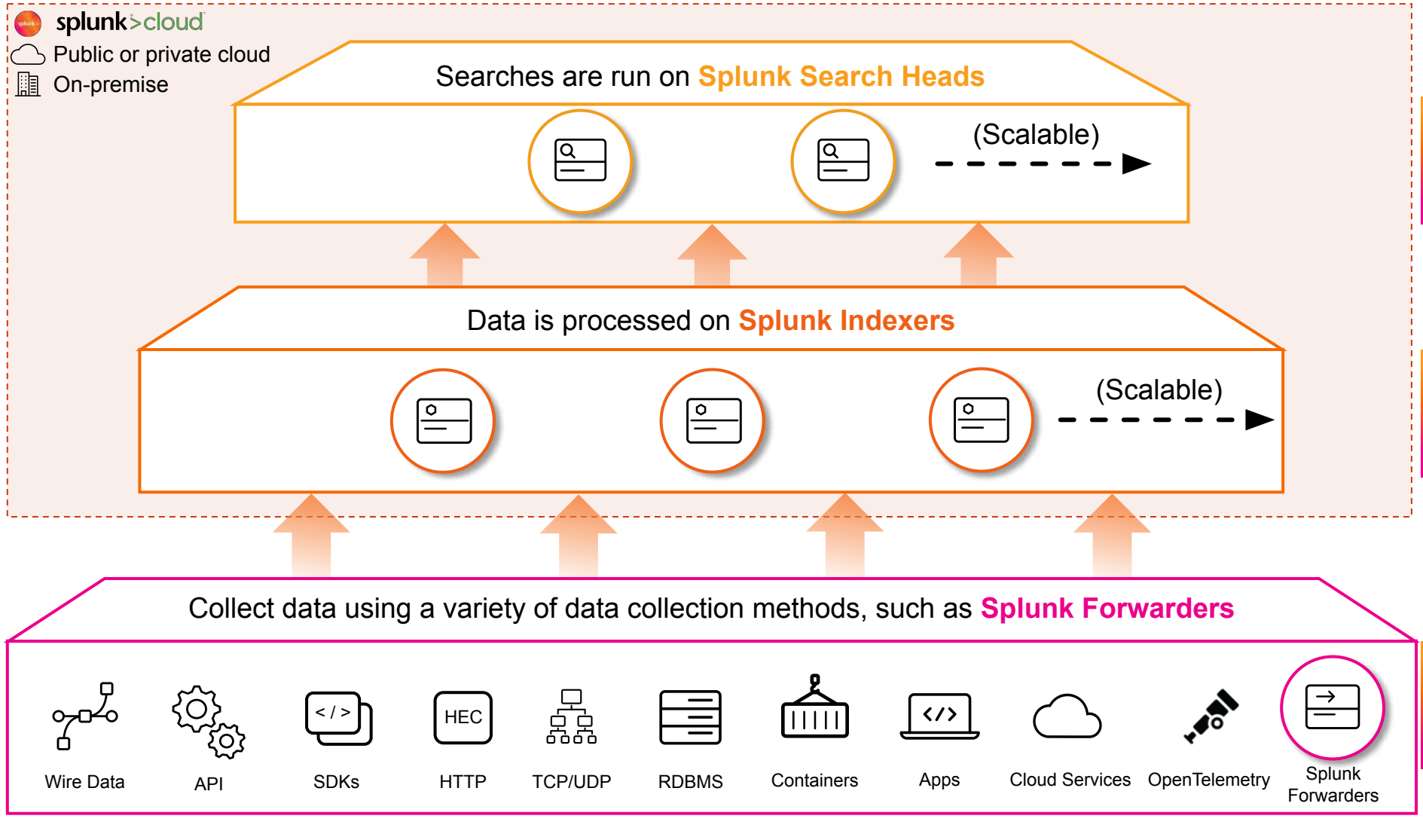
Sample data to play with



Indexer & Search Head combined in a single instance

Scales to Petabytes Per Day

Enterprise-Class Scale, Resilience and Interoperability



- Distribute Searches to Indexers
- Can be clustered (active-active)

- Receive and store raw data
- Data is analysed and indexed
- Can be clustered (active-active)

- Collect/monitor and forward data to Indexers
- Collection options for a variety of data sources

splunk>

What is a Splunk Universal Forwarder?

- Reliable collection of data from remote locations
- Includes methods for collecting from a variety of data sources
- Lightweight but powerful:
  - Buffering / guaranteed delivery
  - Encryption
  - Compression
  - Load balancing
  - And more!
- Very small footprint
- Just forwards data – no parsing beforehand!

Security Data and Searches

For Security People

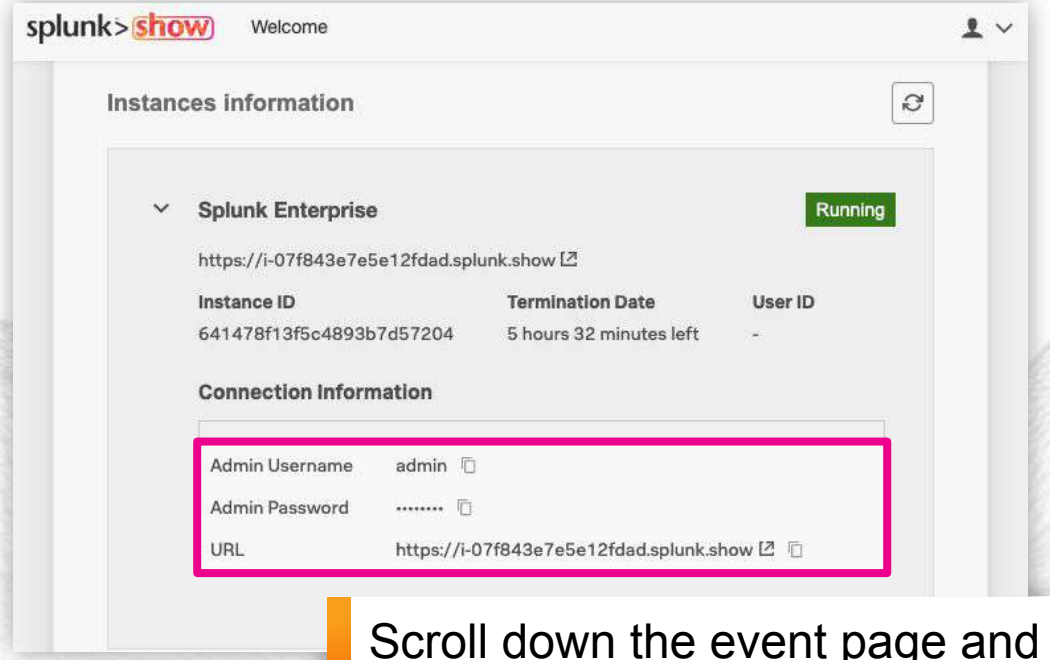
splunk>

Let’s Go!

splunk>

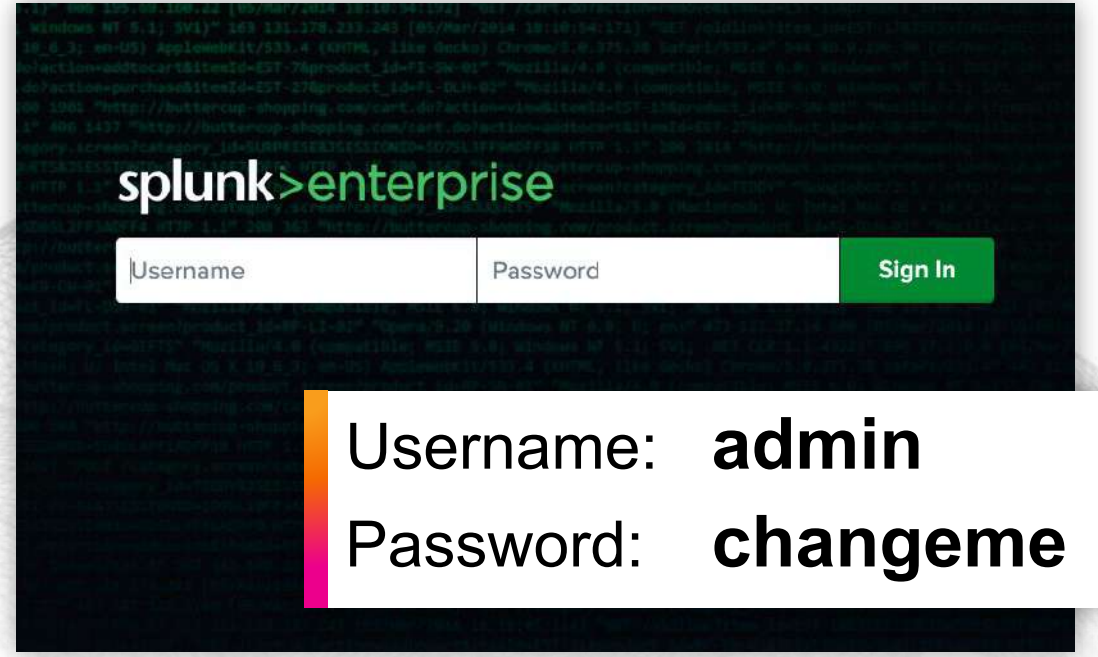
Login to Splunk

Locate your instance URL and credentials in the Splunk Show event https://show.splunk.com



Scroll down the event page and expand the **Splunk Enterprise** section to view your login details

Log in to your Splunk instance



Username: **admin**

Password: **changeme**

splunk>

Search Basics

Using SPL & Navigating the Splunk Search Bar

splunk>

Search Basics

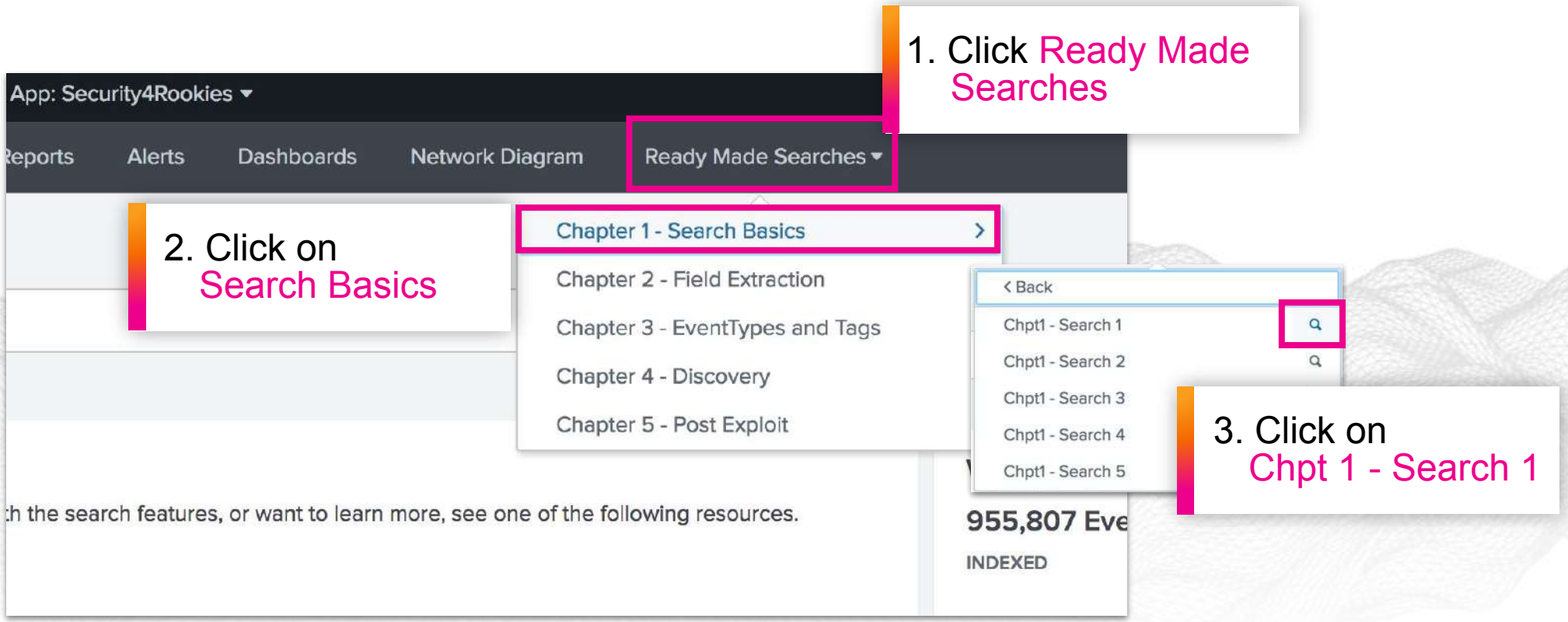
Rules for the Workshop

1. Include or negate with AND or OR
2. Must Capitalize AND / OR
3. Enclose strings in double quotes " " not single ‘ ’
4. Wildcard anywhere
5. CIDR ranges for IP Address matching
6. Keys are case sensitive, values are not

splunk>

The Easy Button

All lab searches have been pre-written for you

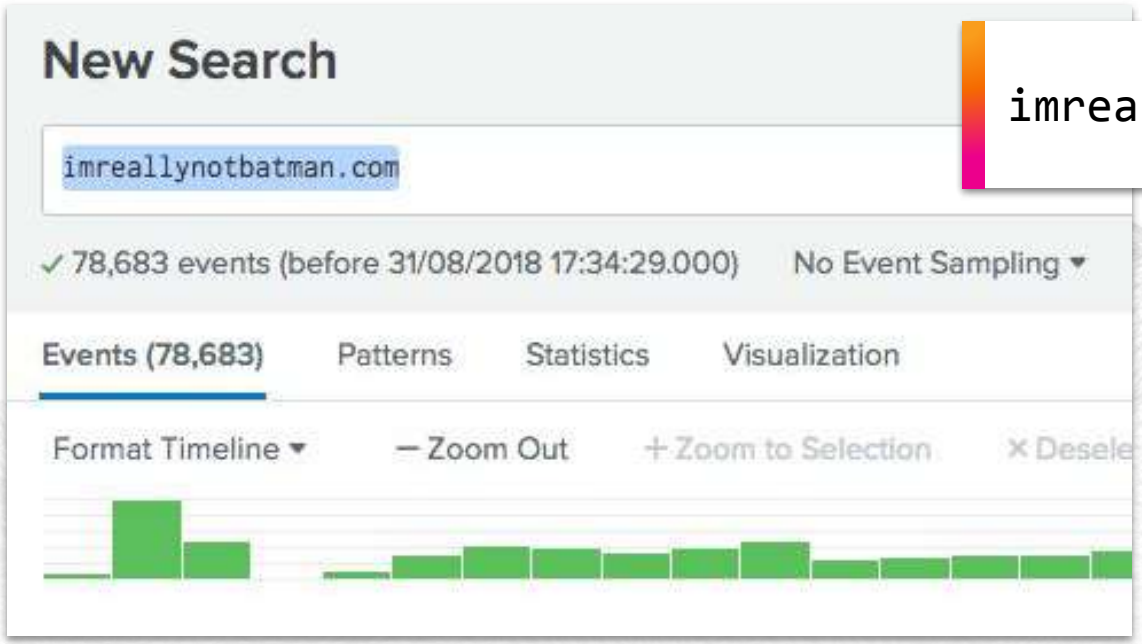


splunk>

Search Basics

Chpt 1 - Search 1

Literal Strings




```
imreallynotbatman.com
```

splunk>

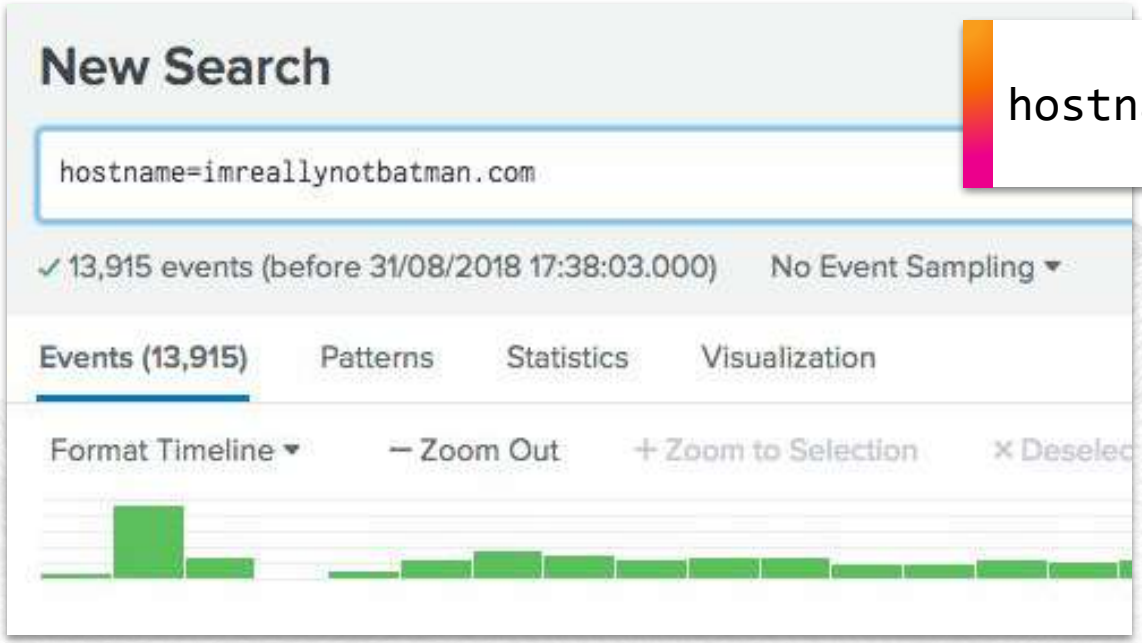
Search Basics

Chpt 1 - Search 2

key=value pair matching

Other Options

=	equals
!=	not equal to
>	greater than
<	less than
>=	greater or equal
<=	less than or equal to




```
hostname=imreallynotbatman.com
```

splunk>

Search Basics

Chpt 1 - Search 3

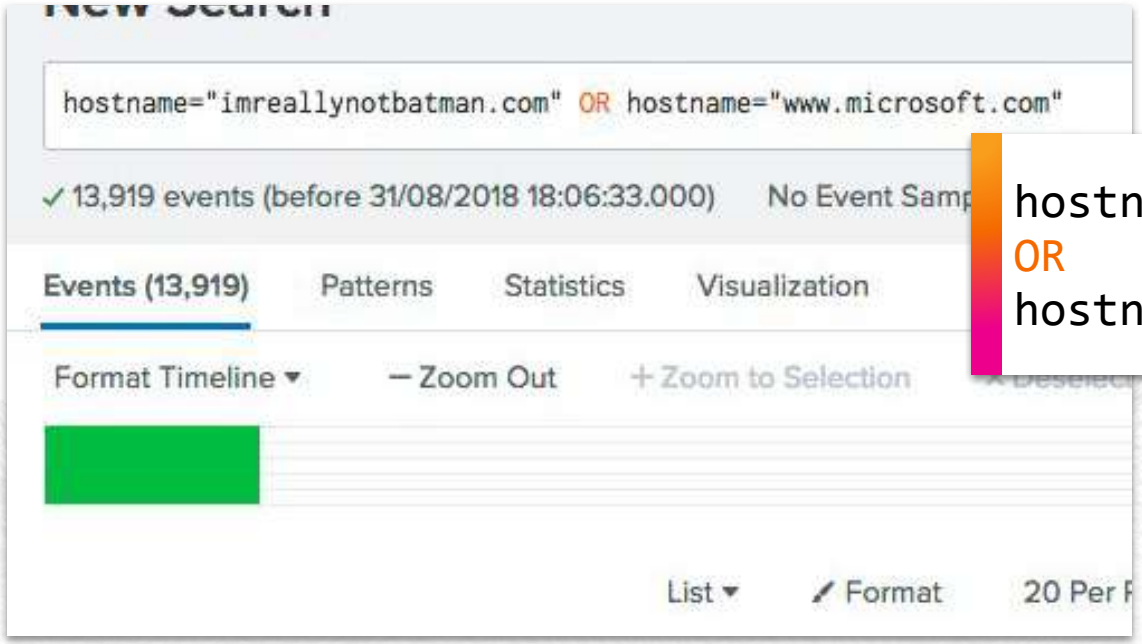
Using OR

Remember Case

hostname=“microsoft.com”

NOT the same as

HOSTNAME=”microsoft.com



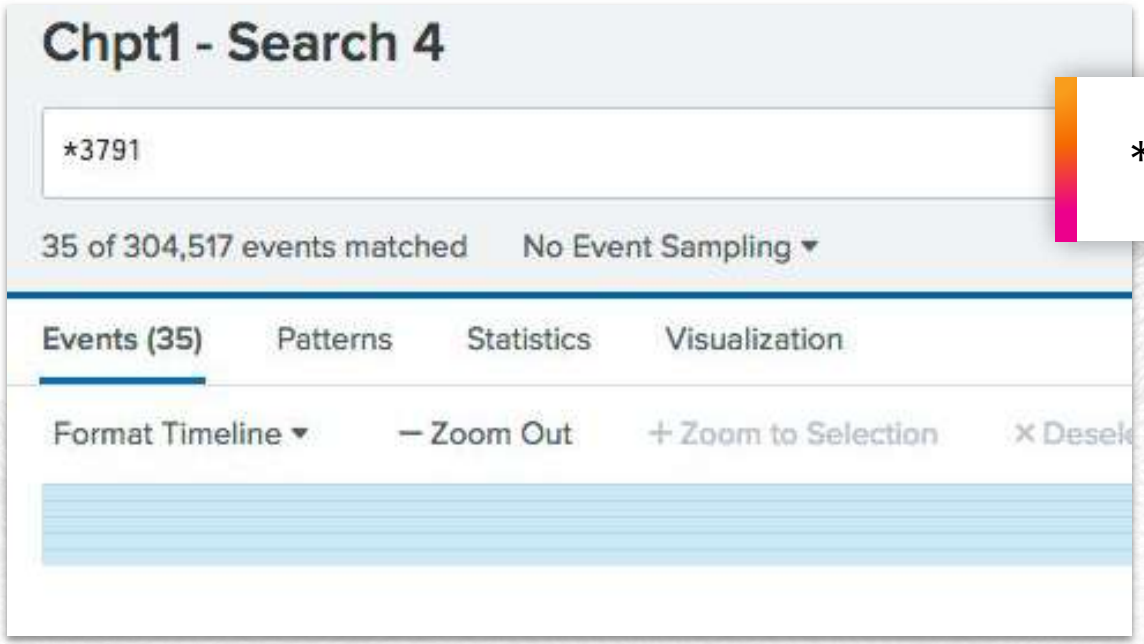

```
hostname=imreallynotbatman.com
OR
hostname="www.microsoft.com"
```

splunk>

Search Basics

Chpt 1 - Search 4

Use Wildcards

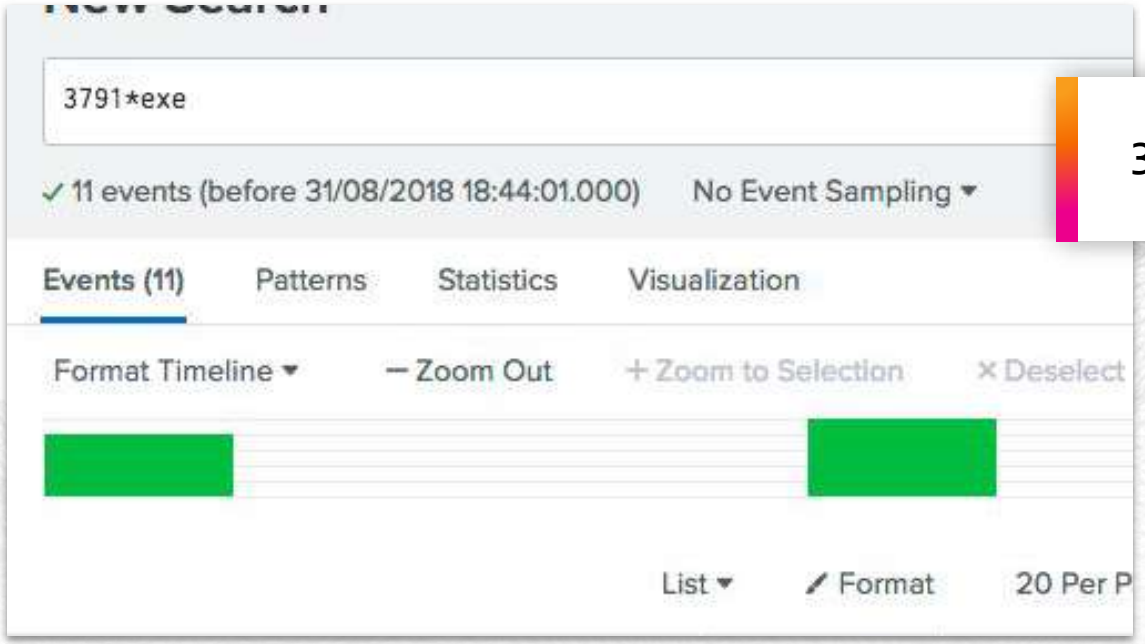


*3791

Search Basics

Chpt 1 - Search 5

Use Wildcards




```
3791*exe
```

Search Basics

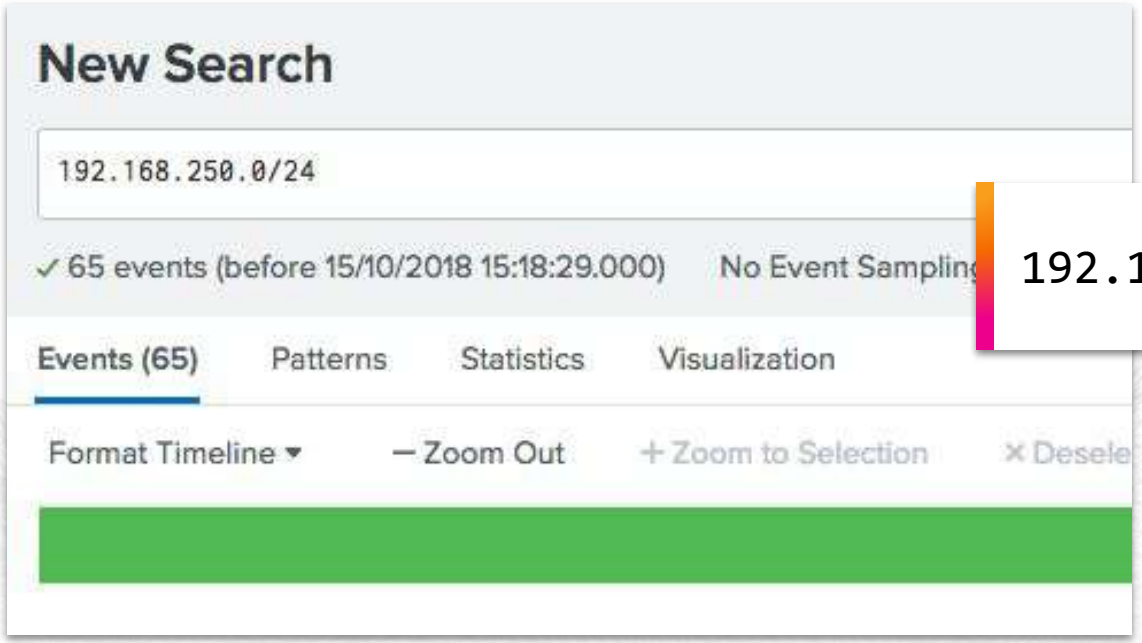
Chpt 1 - Search 6

CIDR Matching

Also an Option

Could also key=value search

dest_ip=192.168.250.0/24



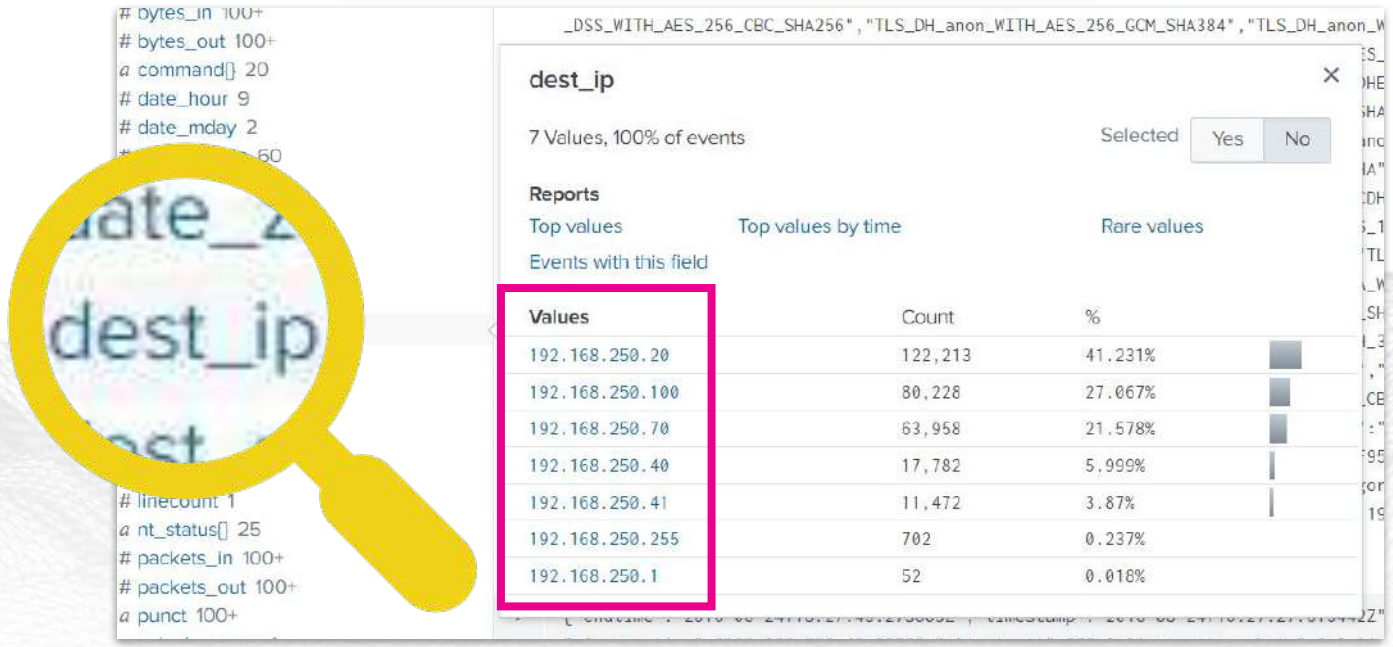
192.168.250.0/24

splunk>

Search Basics

Chpt 1 - Search 6

CIDR Matching



Splunk's Search Processing Language (SPL)

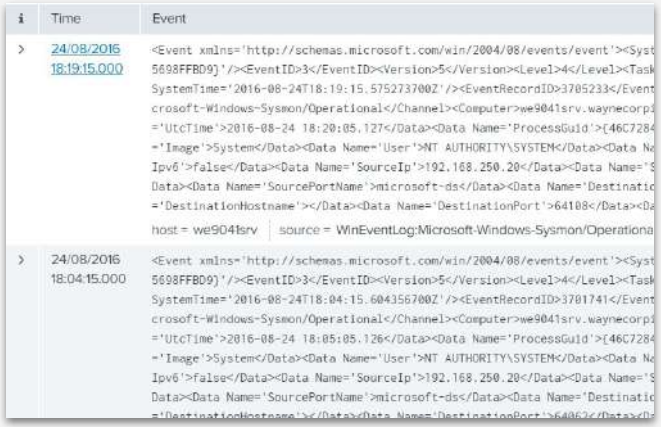
Search Terms **Commands**

```
action=purchase | stats count by src_ip | rename count as requests
```

Pipe character: Output of left is input to right

Functions

e.g. `dest_ip=192.168.250.70`



`| stats count by src_ip`

src_ip	count
108.161.187.134	6
185.10.200.26	5
192.168.2.50	19500
192.168.250.1	17
40.80.148.42	35724

`| rename count as requests`

src_ip	requests
108.161.187.134	6
185.10.200.26	5
192.168.2.50	19500
192.168.250.1	17
40.80.148.42	35724

Want to know more? Check out:
Splunk Quick Reference Guide: https://splk.it/SplunkQuickRef
Search manual: https://splk.it/SplunkSearchManual

Working with statistics? Use stats and functions

Usage

```
<your search> | stats <function> <by clause>
```

Examples

```
sourcetype=access_combined
| stats distinct_count(clientip) by status
```

status	distinct_count(clientip)
200	67
400	67
401	67
402	

Calculates statistics based on fields in your events

```
sourcetype=access_combined
| timechart count by status
```

Creates a time series chart with a corresponding table of statistics

Want to know more? Check out:
Splunk Quick Reference Guide: https://splk.it/SplunkQuickRef

splunk>

Stats Introduction

Examples of stats

```
| stats count
```
Returns the total number of events on 1 line

```
| stats count by src_ip
```
Returns the total number of events per src_ip

```
| stats min(bytes) avg(bytes) max(bytes) by src_ip
```
Returns minimum, average & maximum bytes per src_ip

```
| stats dc(src_ip) by dest_ip
```
Returns the number of (or distinct) src_ips connecting to dest_ip

```
| stats avg(bytes) by _time, src_ip
```
Returns average bytes per time slice and src_ip

splunk>

Indexing Basics

Where the Data Meets Controls

splunk>

Indexing Basic Rules

- Indexes are repositories on your indexer
- A logical way to segregate data
- Access Control is done on Indexes
- Data Retention controlled per Index
- Use them to speed up your searches!

Sourcetype Basics

Where you define the format of your data!

splunk>

Sourcetype Basics

- How Splunk knows where to break events
- How to extract fields from each event
- What data manipulation occurs for each event
- ALL config is stored under the sourcetype name

splunk>

Sourcetype Basics

Examples

```
08/24/2016 12:27:39 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4689
EventType=0
Type=Information
ComputerName=we8105desk.waynecorpinc.local
TaskCategory=Process Termination
OpCode=Info
RecordNumber=39161
Keywords=Audit Success
Message=A process has exited.

Subject:
        Security ID:            NT AUTHORITY\SYSTEM
        Account Name:           WE8105DESK$
        Account Domain:         WAYNECORPINC
        Logon ID:               0x3e7

Process Information:
        Process ID:     0x1030
        Process Name:   C:\Program Files\SplunkUniversalForwarder\bin\splunk-winprintmon.exe
        Exit Status:    0x1
```

WinEventLog:Security

Multi Line Breaking
Complex Field Extractions
Process ID needs Hex Decoding

```
Aug 24 12:27:14 192.168.250.1 date=2016-08-24 time=12:27:14 devname=gotham-fortigate devid=FGT60D4614044725 logid=1059028704 type=utm subtype=app-ctrl
 eventtype=app-ctrl-all level=information vd="root" appid=16270 user="" srcip=192.168.250.41 srcport=51108 srcintf="internal3" dstip=91.189.91.157 dst
port=123 proto=17 service="NTP" policyid=10 sessionid=4237590 applist="Honeypot-Access" appcat="Network.Service" app="NTP" action=pass msg="Network.Se
rvice: NTP," apprisk=elevated
```

fortigate:utm

Single Line Breaking
Key=Value pair Extractions

splunk>

Extracting Fields Basics

Where you make your data useable

splunk>

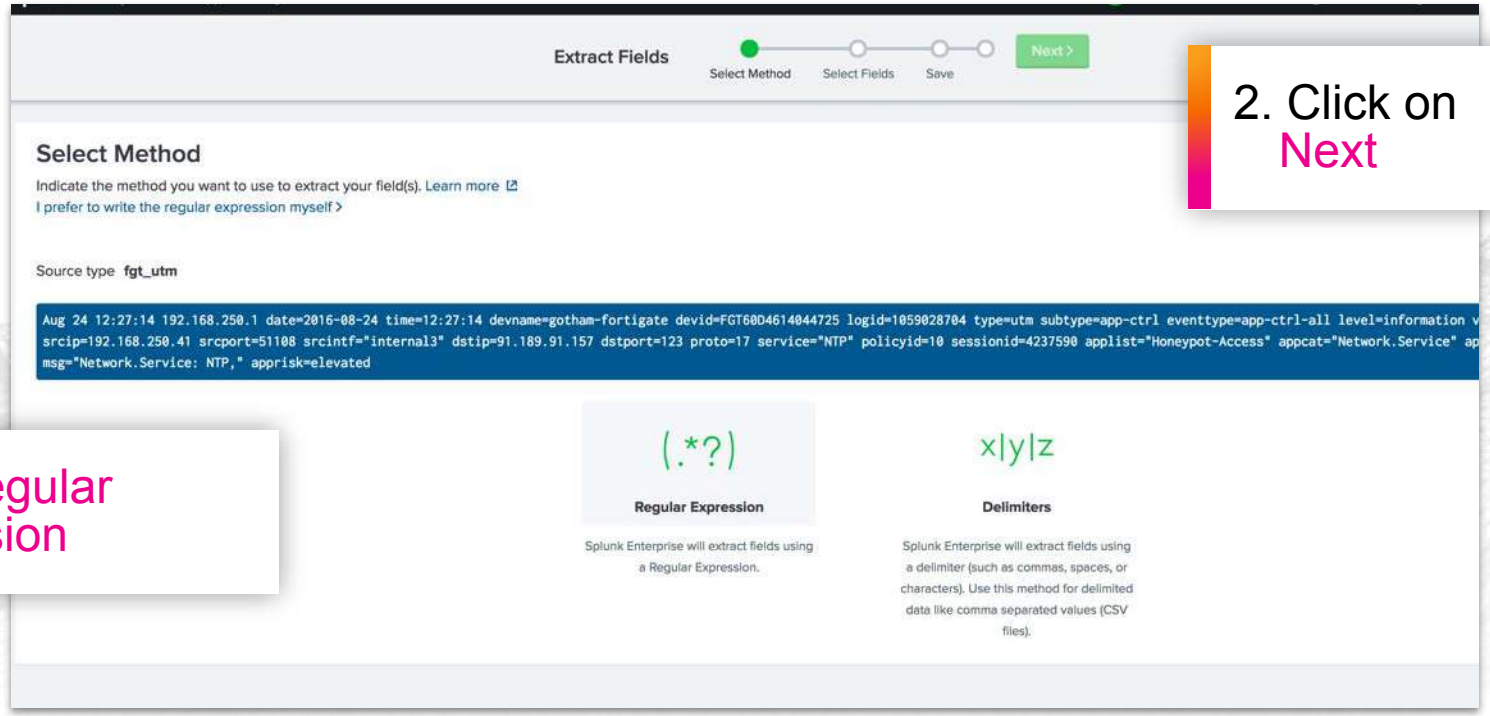
Field Extraction Basics

- Technology Add-ons (TA) are your fastest route
  - splunkbase.splunk.com – search “Technology Add-on”
- Check automatically recognized sourcetypes
  - http://docs.splunk.com/Documentation/Splunk/latest/Data/Listofpretrainedsourcetypes
- Key=Value works out the box – use field aliasing if you want to rename
- UI based extraction when 1 – 3 didn’t come through for you

Field Extraction

Chpt 2 - Search 1

Extract a Field



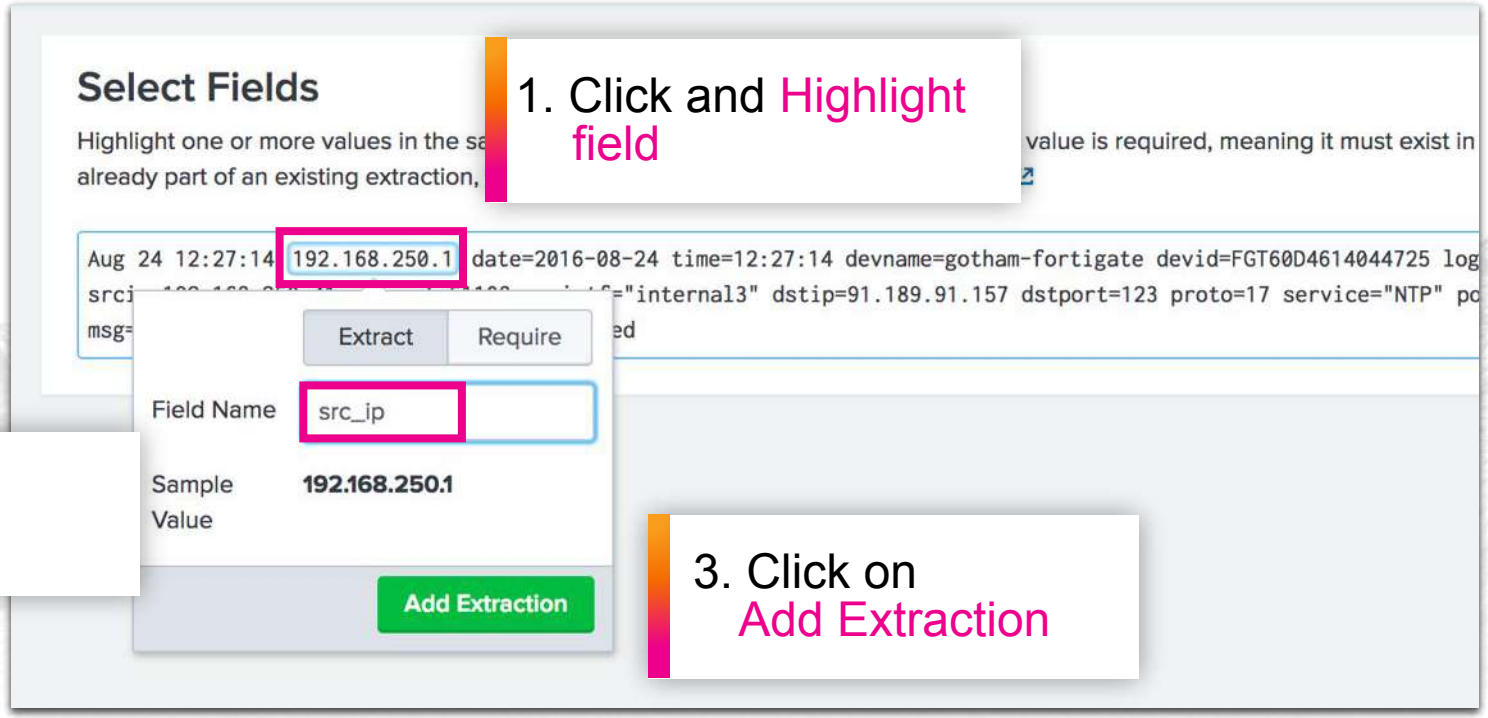
1. Click Regular Expression

2. Click on Next

Field Extraction

Chpt 2 - Search 1

Highlight and Name



1. Click and Highlight field

2. Enter src_ip

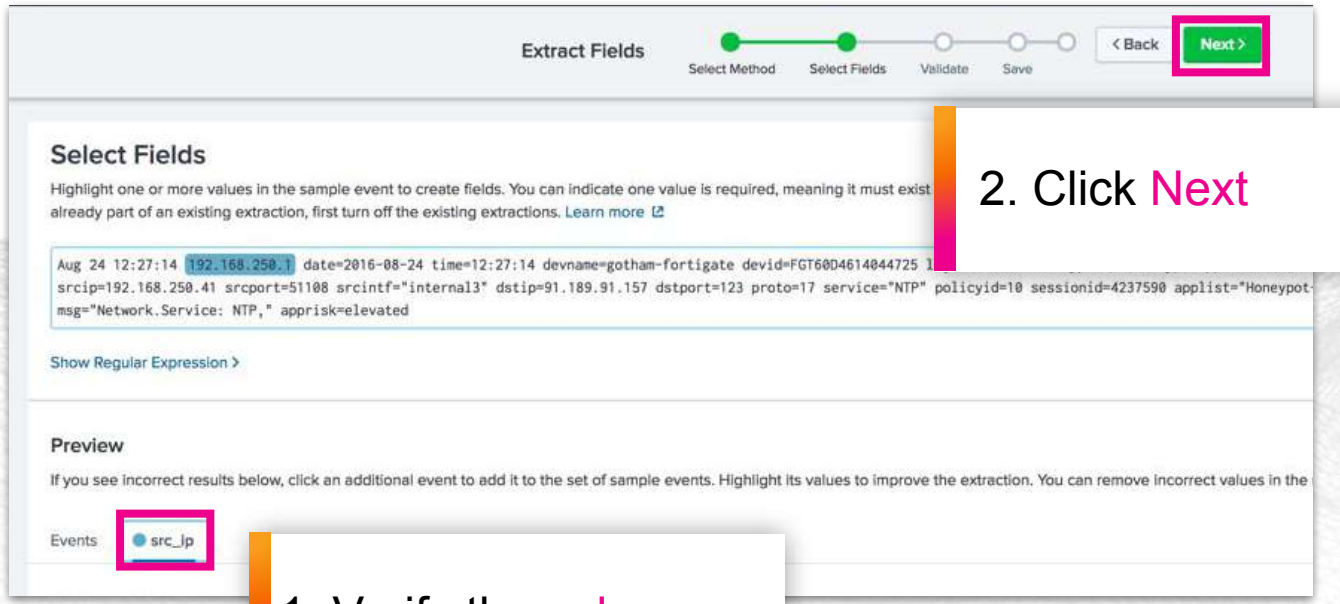
3. Click on Add Extraction

splunk>

Field Extraction

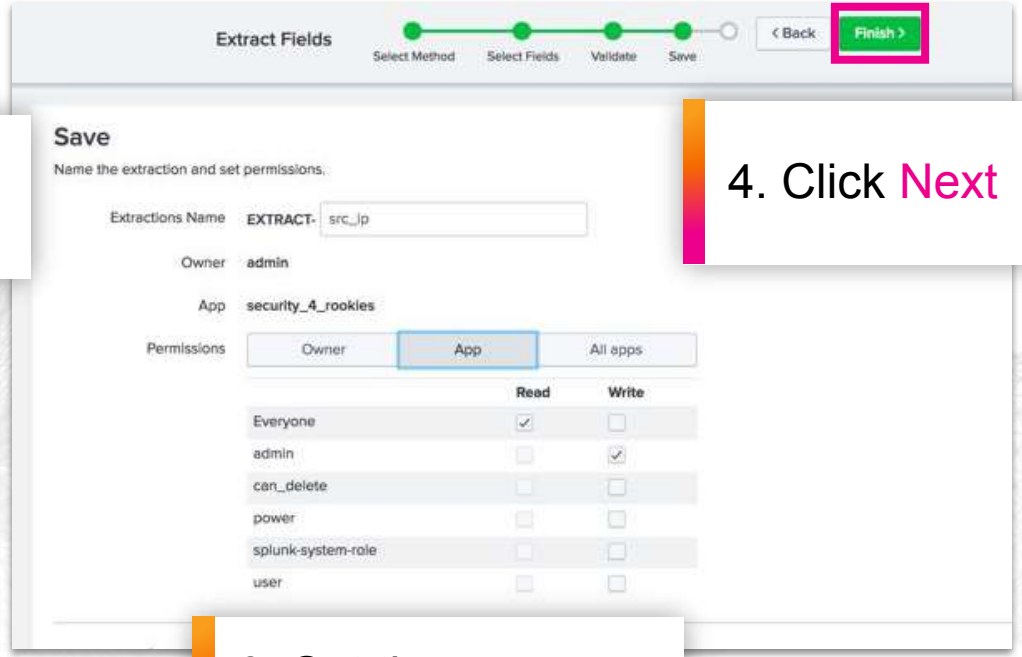
Chpt 2 - Search 1

Verify Field and Set Access



2. Click Next

1. Verify the values



4. Click Next

3. Set the Permissions

splunk>

Event Types & Tags Basics

Where you make correlated data scale

splunk>

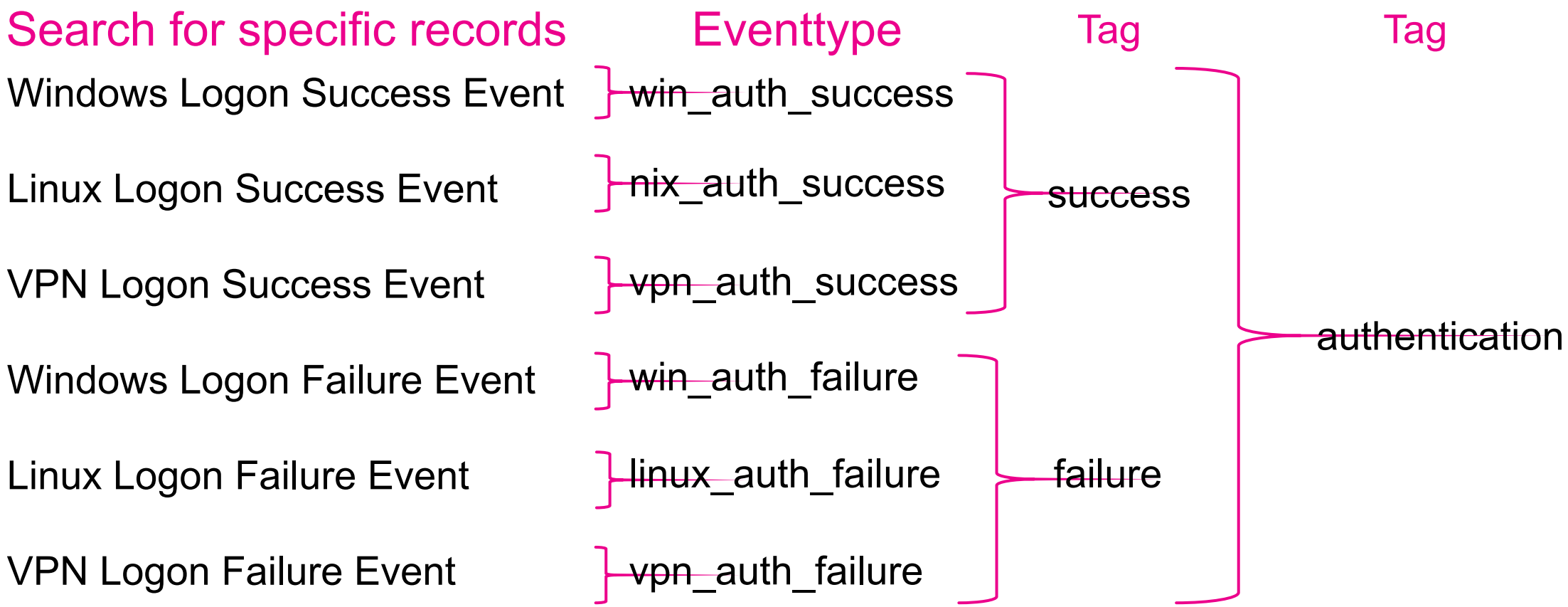
Event Types & Tags Basics

- Event types are created to categorize specific events within a sourcetype
- Tags are abstractions over the top of event types

splunk>

Correlating Events

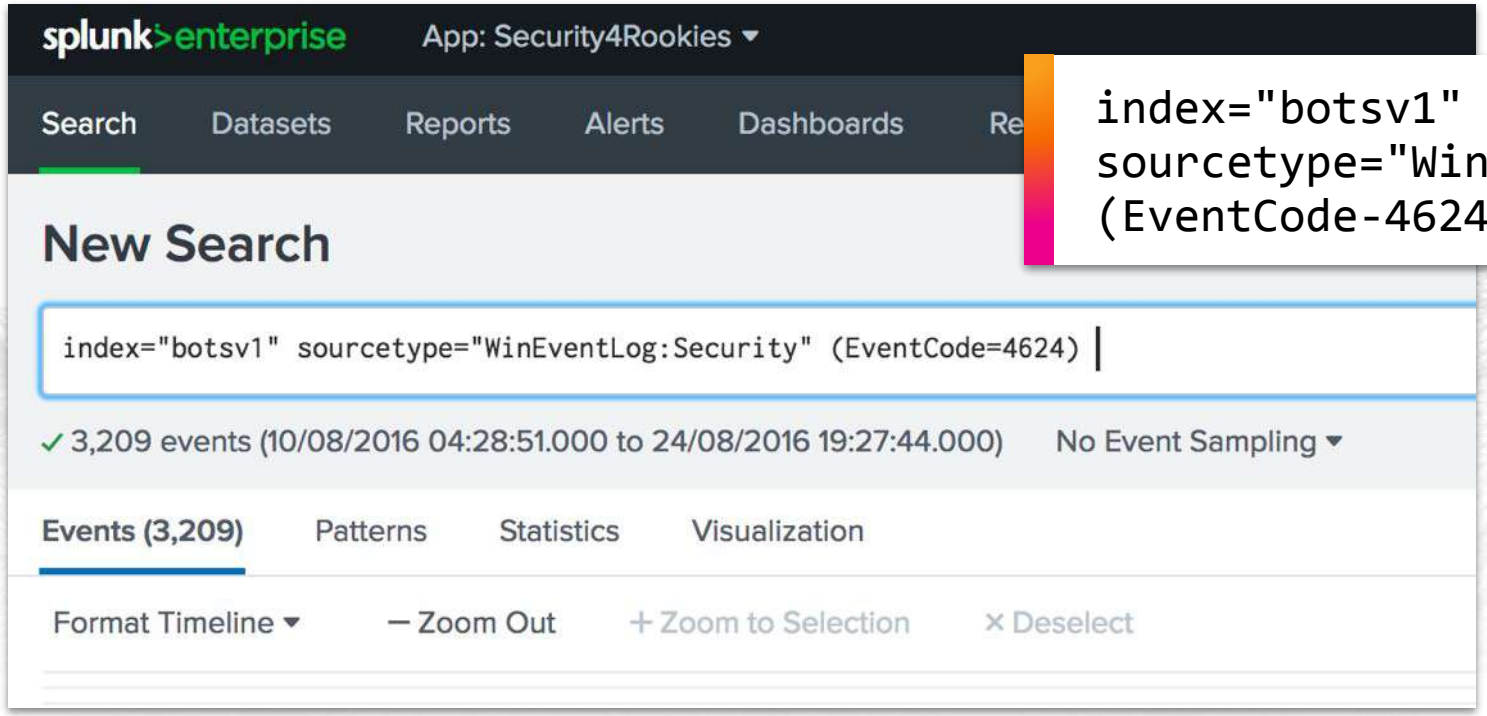
Using EventTypes and Tags



Eventtypes and Tags

Chpt 3 - Search 1

Creating an eventtype




```
index="botsv1"
sourcetype="WinEventLog:Security"
(EventCode-4624)
```

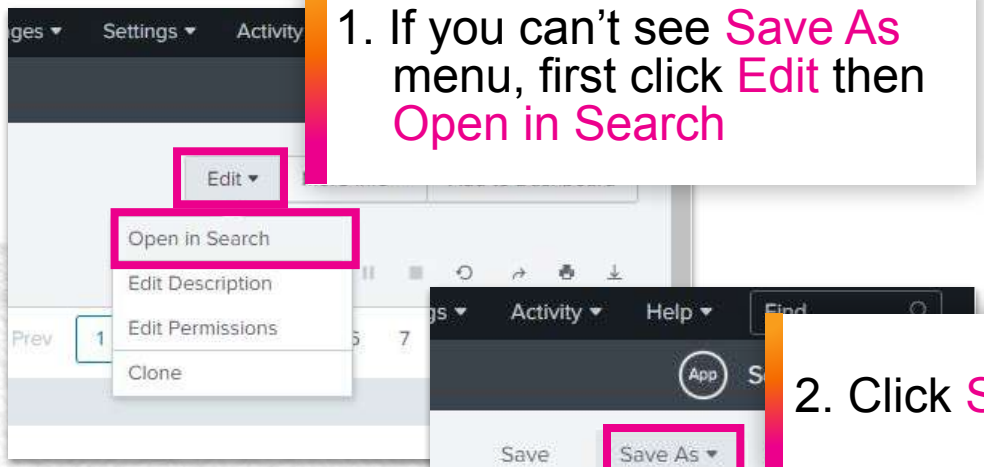
splunk>

Eventtypes and Tags

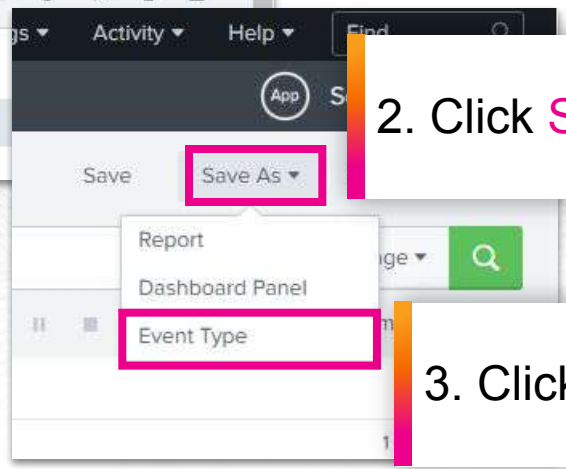
Chpt 3 - Search 1

Creating an eventtype

1. If you can't see Save As menu, first click Edit then Open in Search

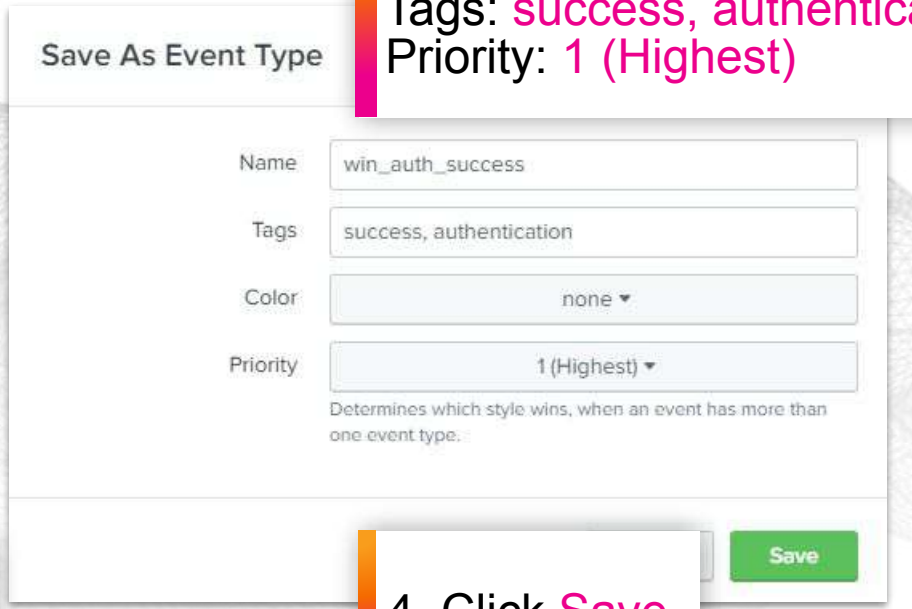


2. Click Save As



3. Click Event Type

Name: win_auth_success
Tags: success, authentication
Priority: 1 (Highest)



4. Click Save

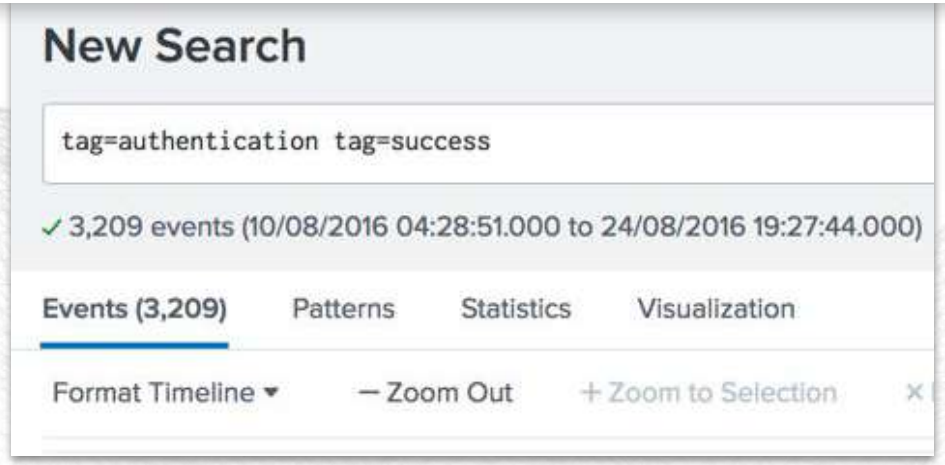
splunk>

Eventtypes and Tags

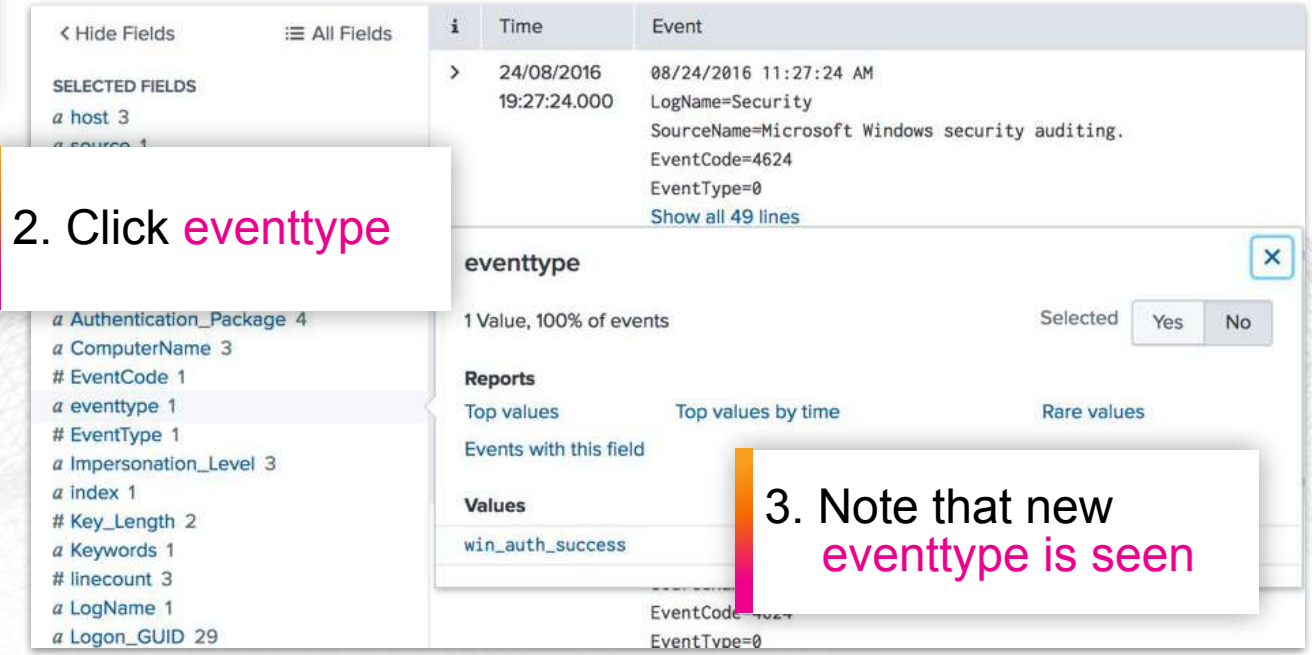
Chpt 3 - Search 2

Searching by Tags

1. Enter
   `tag=authentication tag=success`



2. Click eventtype



3. Note that new eventtype is seen

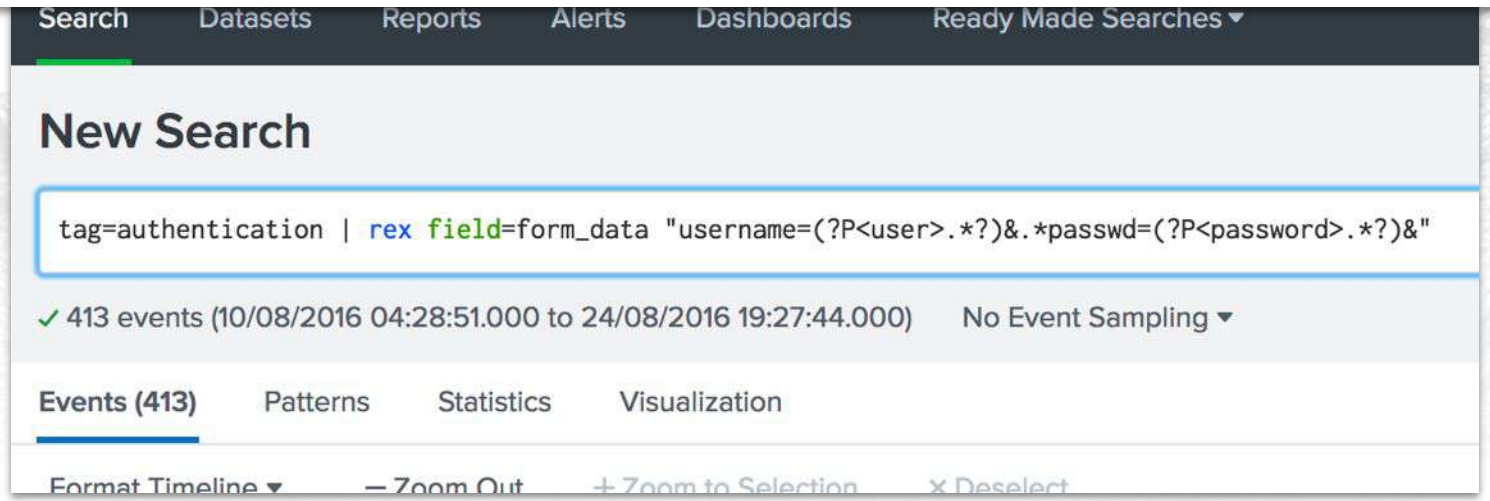
Bonus Material

Chpt 3 - Search 3

REGEX for the brave

```
                                | rex field=<field_name> "(?P<>)"

| rex field=<field_name> "beforepattern(?P<extract_name>field_match)afterpattern"
```



splunk>

Break Time

15 min refuel

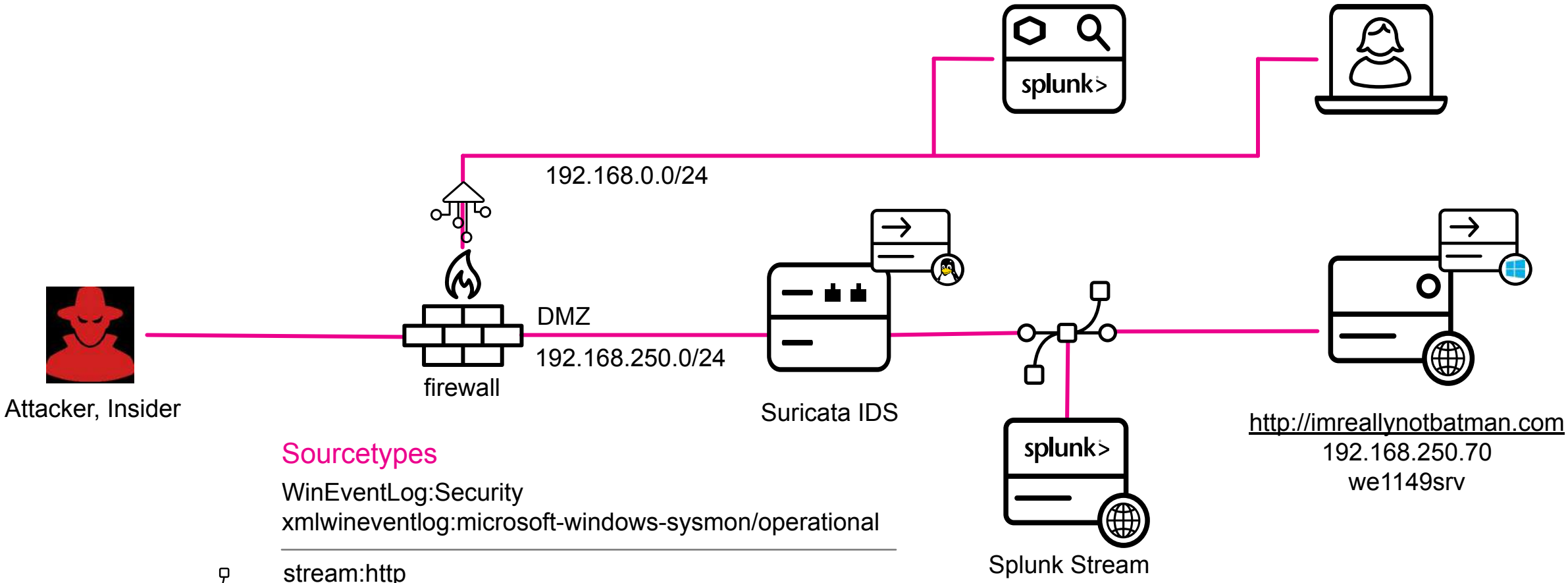
splunk>

Security Data and Searches

For Security People

splunk>

WayneCorp Network



Sourcetypes

WinEventLog:Security
xmlwineventlog:microsoft-windows-sysmon/operational

---

wire data

stream:http
stream:dns
stream:*

---

firewall

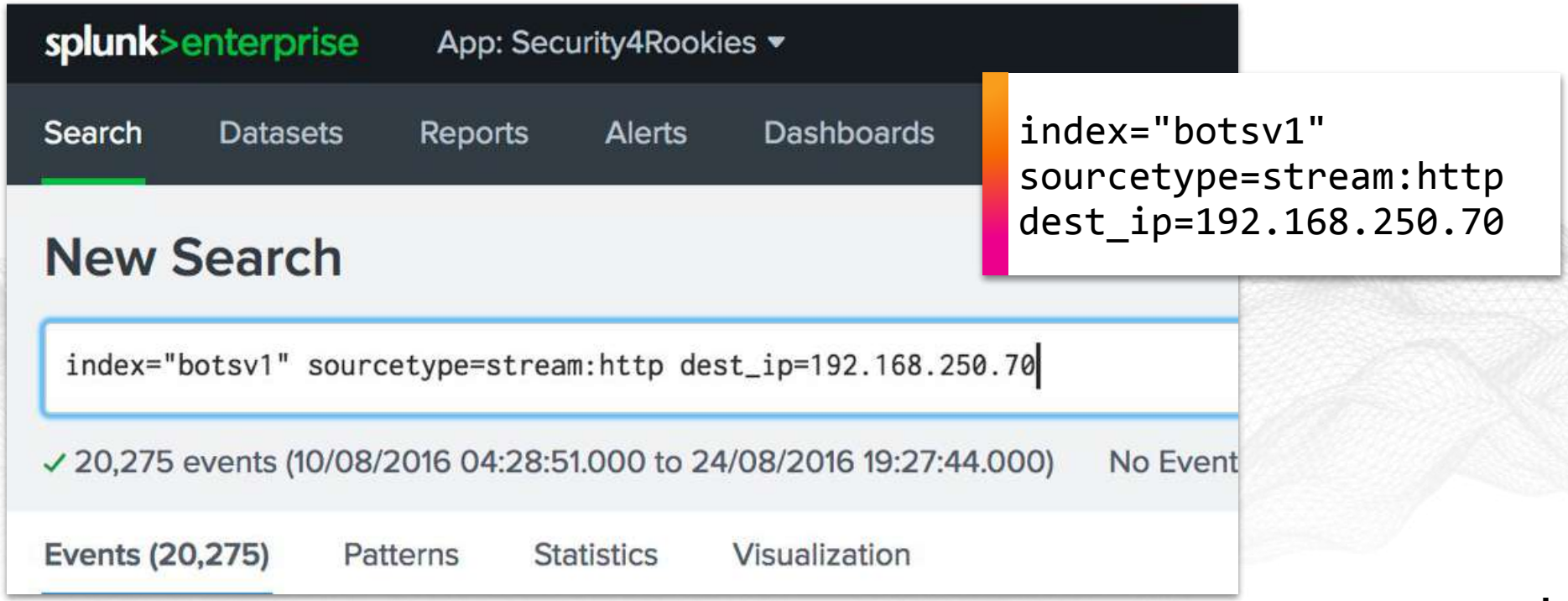
fgt_utm

splunk>

Discovering the Attack

Chpt 4 - Search 1

Filter Traffic to the Web Server

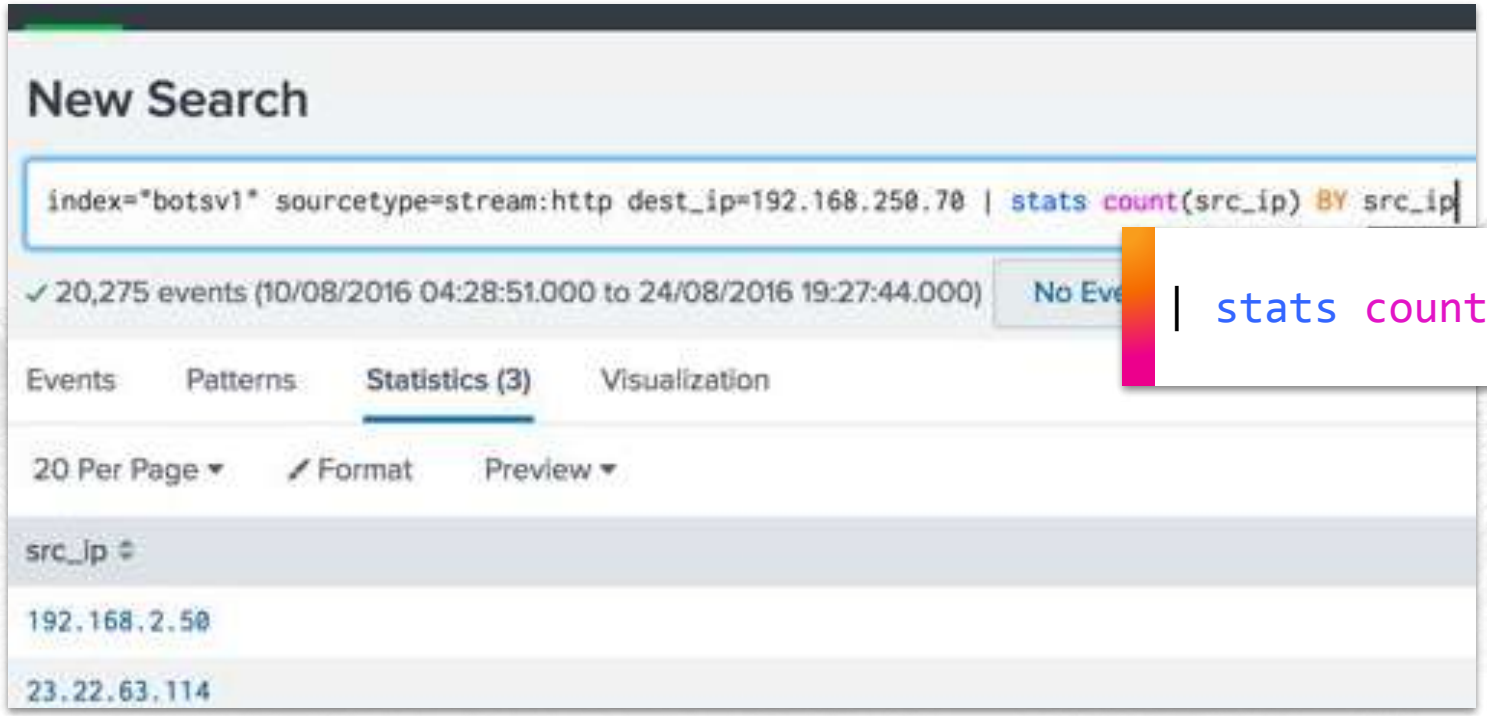


splunk>

Discovering the Attack

Chpt 4 - Search 2

Use stats to Aggregate




```
| stats count(src_ip) by src_ip
```

splunk>

Discovering the Attack

Chpt 4 - Search 3

Rename Fields on the Fly


```
| stats count(src_ip) AS requests BY src_ip
```

New Field

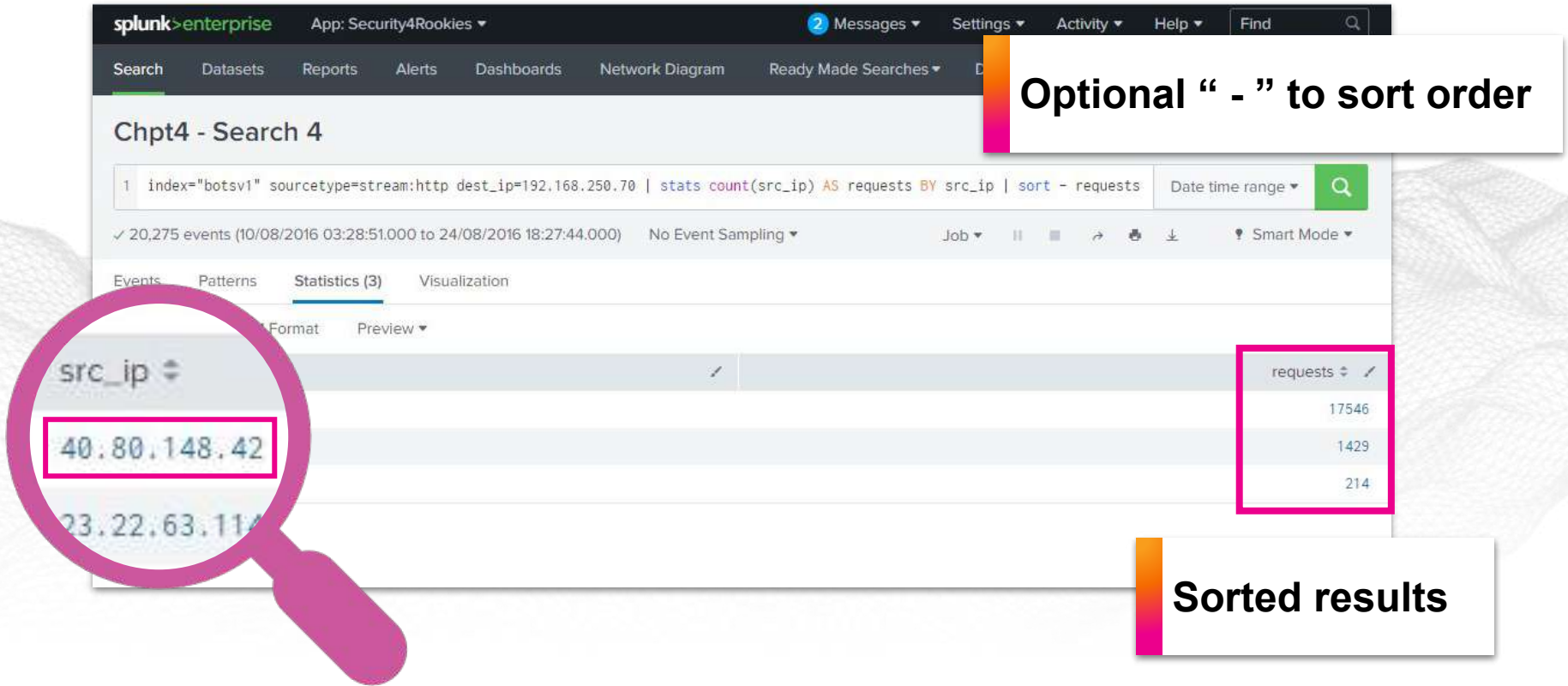
requests
214
1429
17546

splunk>

Discovering the Attack

Chpt 4 - Search 4

Using the sort Command

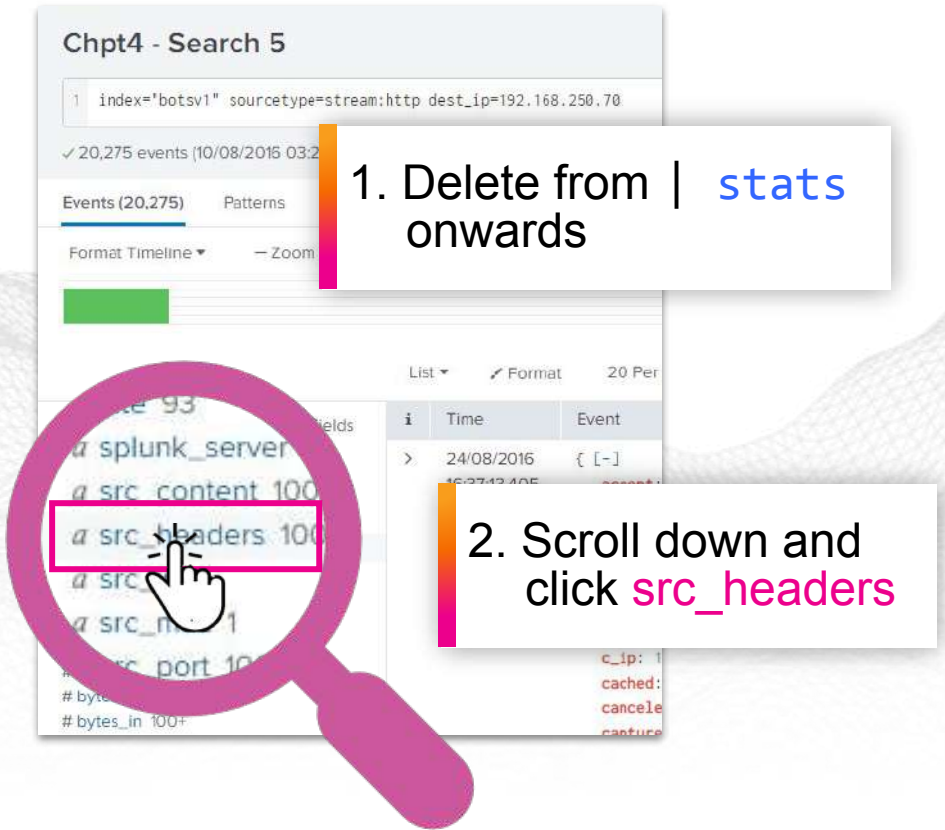


splunk>

Discovering the Attack

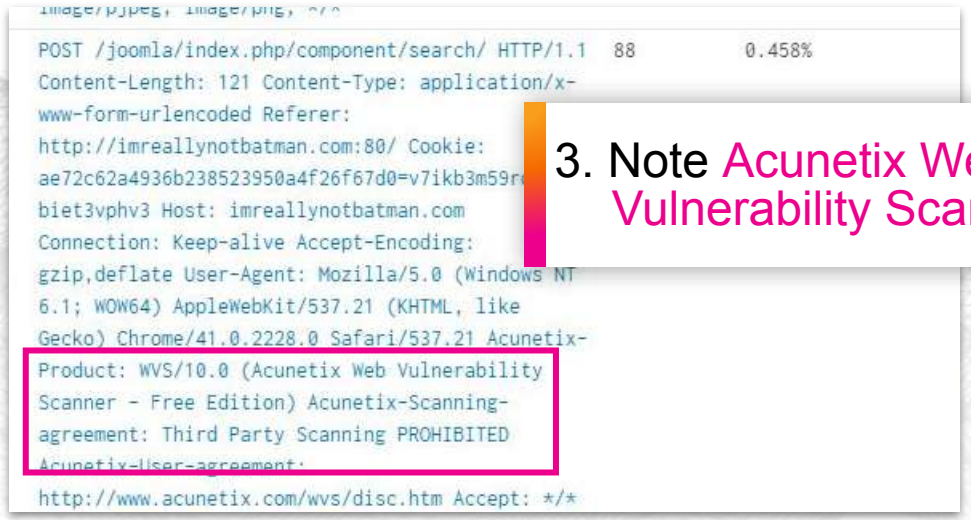
Chpt 4 - Search 5

Investigate the Source Headers



1. Delete from | `stats` onwards

2. Scroll down and click src_headers



3. Note Acunetix Web Vulnerability Scanner

splunk>

Discovering the Attack

Chpt 4 - Search 6

Investigate the Traffic


```
index="botsv1" sourcetype=stream:http dest_ip=192.168.250.70
| stats count(src_ip) AS requests BY src_ip, http_method
| sort - requests
```

splunk>

Discovering the Attack

Chpt 4 - Search 7

Investigate Data Being Received

1. Page through to see acunetix web vulnerability scanning and other bad things!

```
index="botsv1"
sourcetype=stream:http
dest_ip=192.168.250.70
src_ip=40.80.148.42
http_method="POST"
| stats count BY form_data
```

splunk>

Discovering the Attack

Chpt 4 - Search 8

Investigate Login Activity


```
index="botsv1"
sourcetype=stream:http
form_data=*username*passwd*
```

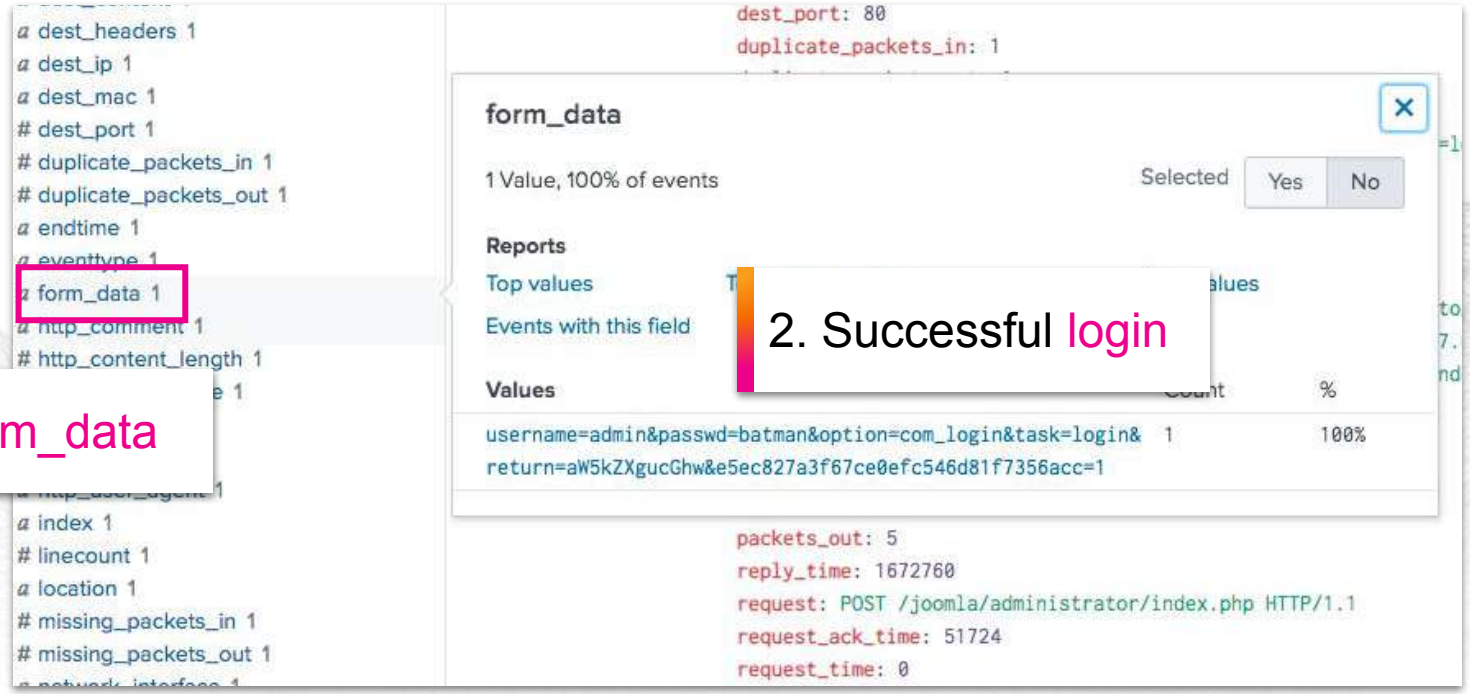
Admin user being brute forced

splunk>

Discovering the Attack

Chpt 4 - Search 9

Inspect the login activity



1. Click form_data

2. Successful login

Unauthorized Access

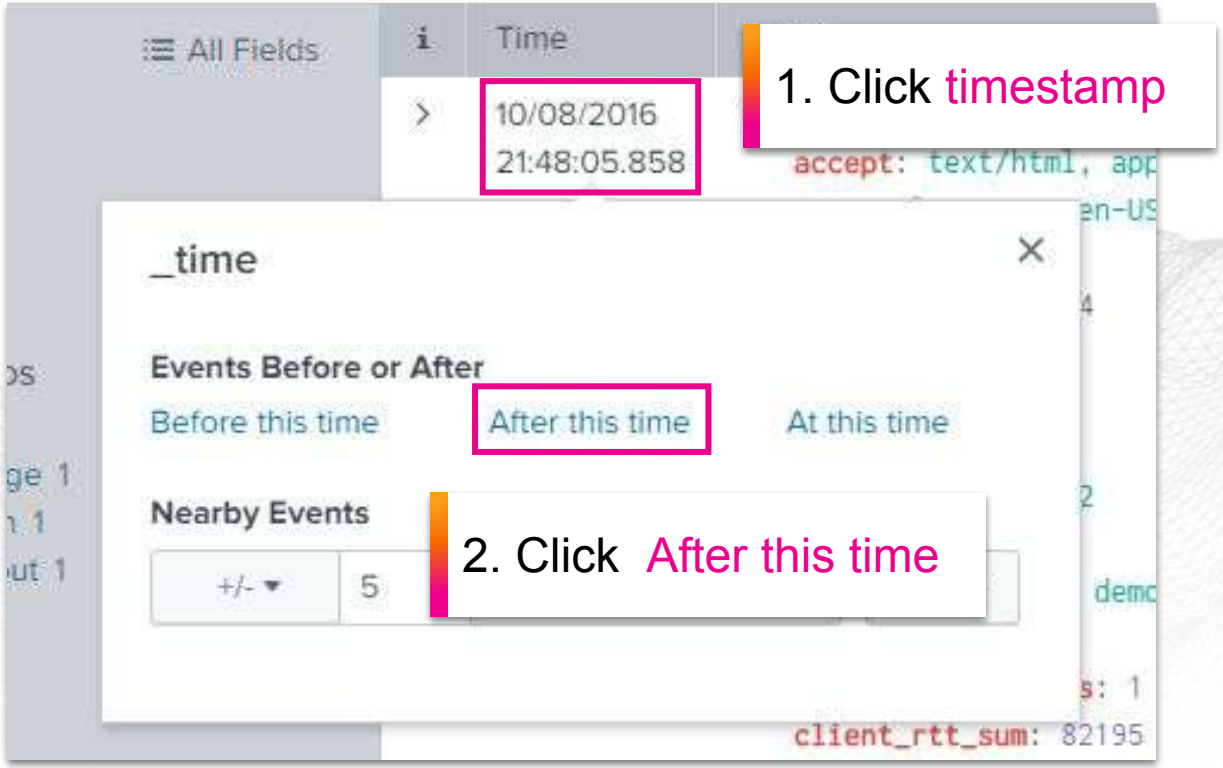
What happened next

splunk>

Post Exploit

Scene Setting

Set the time range

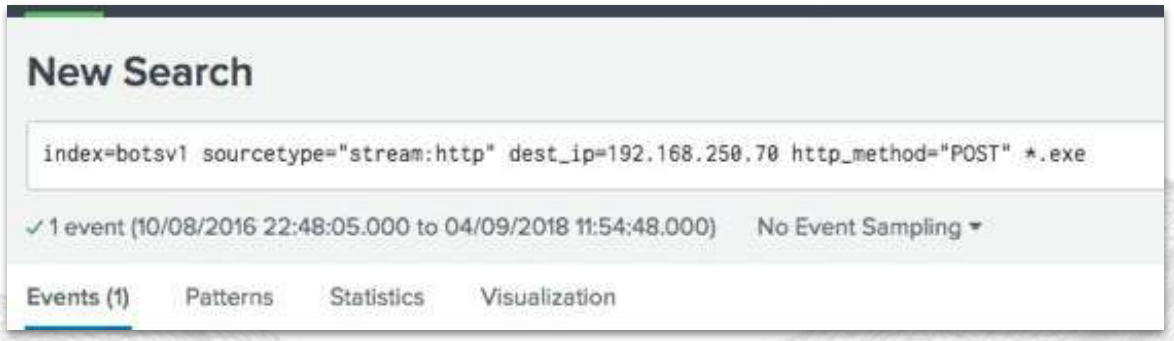


splunk>

Post Exploit

Chpt 5 - Search 1

Looking for a Dropper File




```
index="botsv1"
sourcetype=stream:http
dest_ip=192.168.250.70
http_method="POST"
*.exe
```

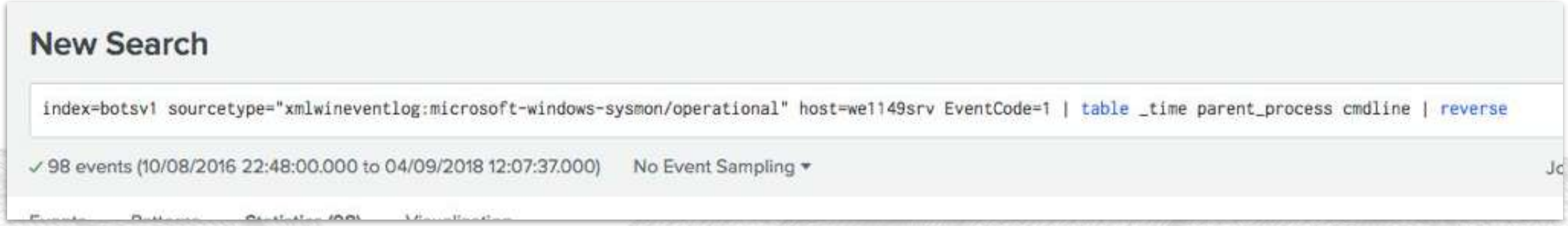
Executable uploaded

splunk>

Post Exploit

Chpt 5 - Search 2

Investigate Endpoint Process




```
index="botsv1"
sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational"
host=we1149srv
EventCode=1
| table _time parent_process cmdline
| reverse
```

splunk>

Post Exploit

Chpt 5 - Search 2

Investigate Endpoint Process

_time	parent_process	cmdline
2016-08-10 23:19:14	C:\Program Files (x86)\PHP\v5.5\php-cgi.exe	cmd.exe /c "dir 2>&1"
2016-08-10 23:19:14	C:\Windows\SysWOW64\cmd.exe	\??\C:\Windows\system32\conhost.exe 0xffffffff
2016-08-10 23:19:22	C:\Program Files (x86)\PHP\v5.5\php-cgi.exe	cmd.exe /c "dir 2>&1"
2016-08-10 23:19:22	C:\Windows\SysWOW64\cmd.exe	\??\C:\Windows\system32\conhost.exe 0xffffffff
2016-08-10 23:19:48	C:\Program Files (x86)\PHP\v5.5\php-cgi.exe	cmd.exe /c "dir 2>&1"
2016-08-10 23:19:48	C:\Windows\SysWOW64\cmd.exe	\??\C:\Windows\system32\conhost.exe 0xffffffff
2016-08-10 23:20:10	C:\Program Files (x86)\PHP\v5.5\php-cgi.exe	cmd.exe /c "move ..\1.jpeg 2.jpeg 2>&1"
2016-08-10 23:20:10	C:\Windows\SysWOW64\cmd.exe	\??\C:\Windows\system32\conhost.exe 0xffffffff
2016-08-10 23:20:13	C:\Program Files (x86)\PHP\v5.5\php-cgi.exe	cmd.exe /c "dir 2>&1"
2016-08-10 23:20:13	C:\Windows\SysWOW64\cmd.exe	\??\C:\Windows\system32\conhost.exe 0xffffffff
2016-08-10 23:20:33	C:\Program Files (x86)\PHP\v5.5\php-cgi.exe	cmd.exe /c "move 2.jpeg imnotbatman.jpg 2>&1"

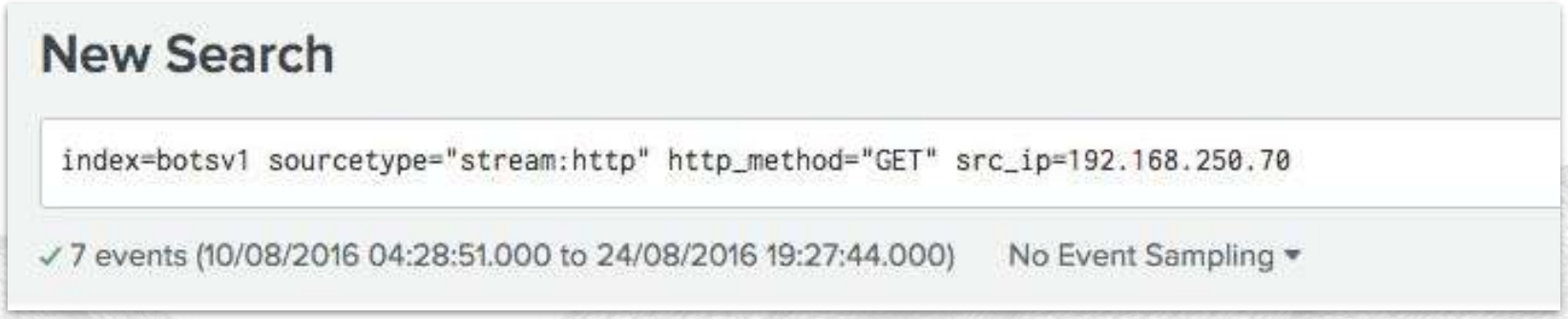
imnotbatman.jpg Overwritten!

splunk>

Post Exploit

Chpt 5 - Search 3

Investigate Web Server Activity



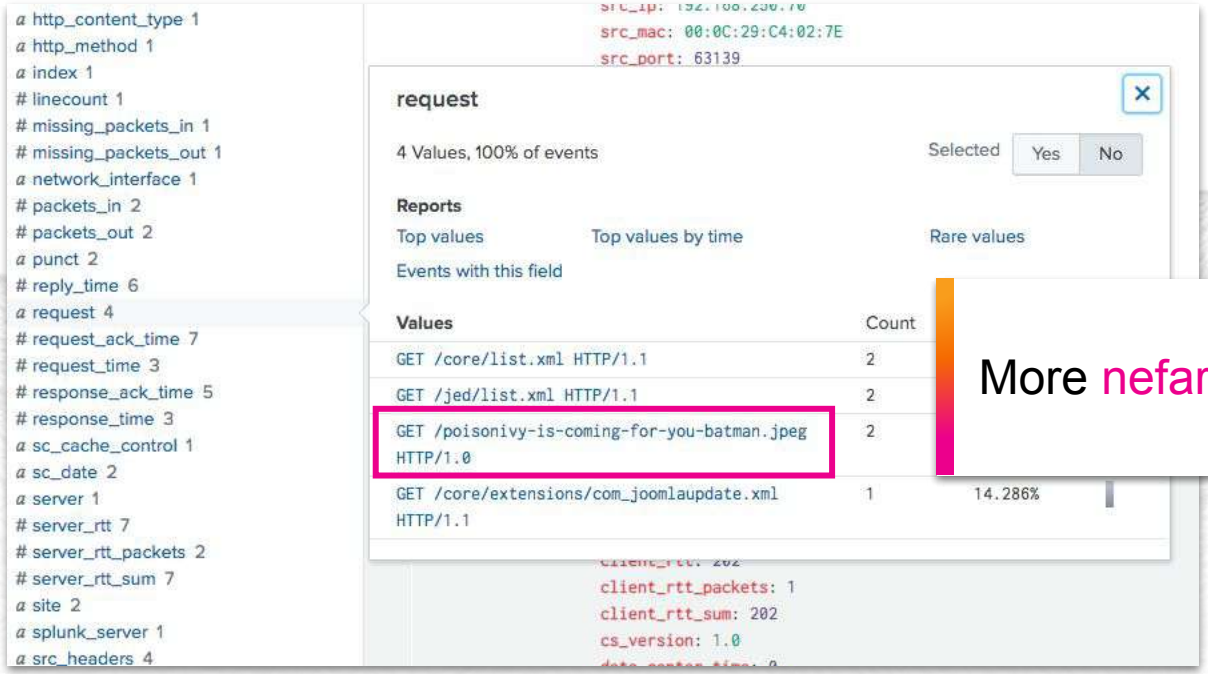

```
index="botsv1"
sourcetype=stream:http
http_method="POST"
src_ip=192.168.250.70
```

splunk>

Post Exploit

Chpt 5 - Search 3

Investigate Web Server Activity



More nefarious behaviour

Post Exploit

Chpt 5 - Search 3

Investigate Web Server Activity

1. Fetching the jpeg

2. DDNS Site

splunk>

Dashboards

My Manager wants them now! - OK

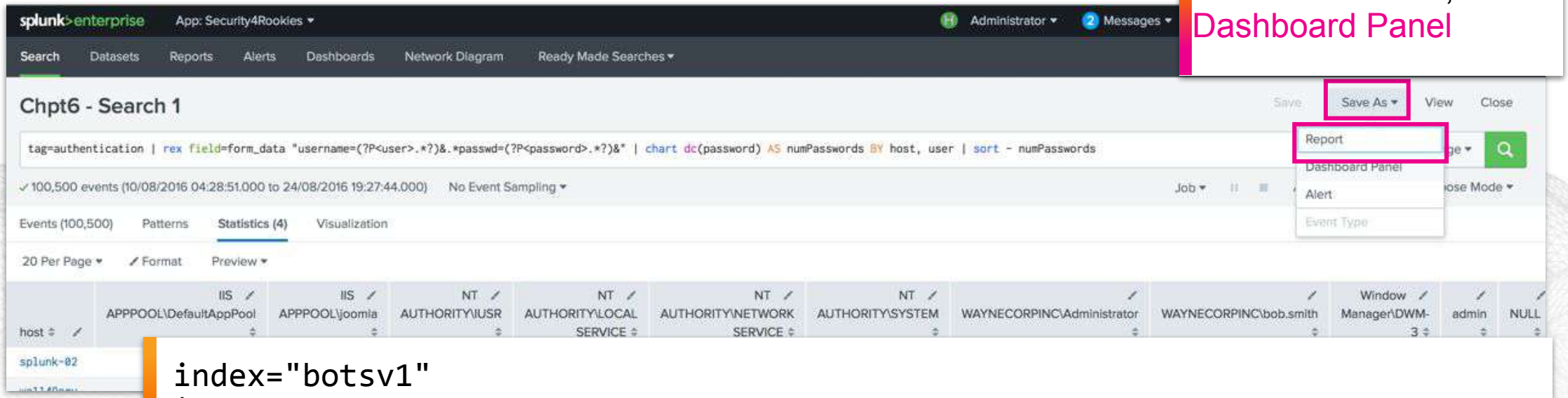
splunk>

Dashboards

Chpt 6 - Search 1

Brute Force Activity

2. Click Save As, then Dashboard Panel



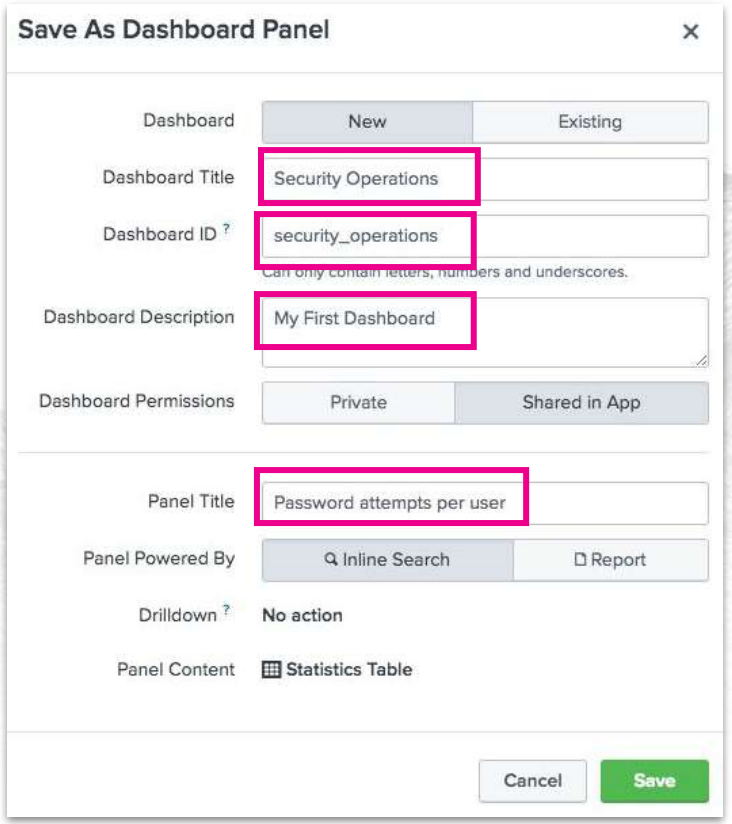

```
index="botsv1"
| rex field=form_data "username=(?P<user>.*?)&.*passwd=(?<password>.*?)&"
| chart dc(password) AS numPasswords BY host, user
| sort - numPasswords
```

Dashboards

Chpt 6 - Search 1

Brute Force Activity

1. Click New



Dashboard Title: Security Operations
Dashboard ID: security_operations
Dashboard Desc: My First Dashboard
Panel Title: Password attempts per user

splunk>

Dashboards

Chpt 6 - Search 2

Unexpected Logon Sources

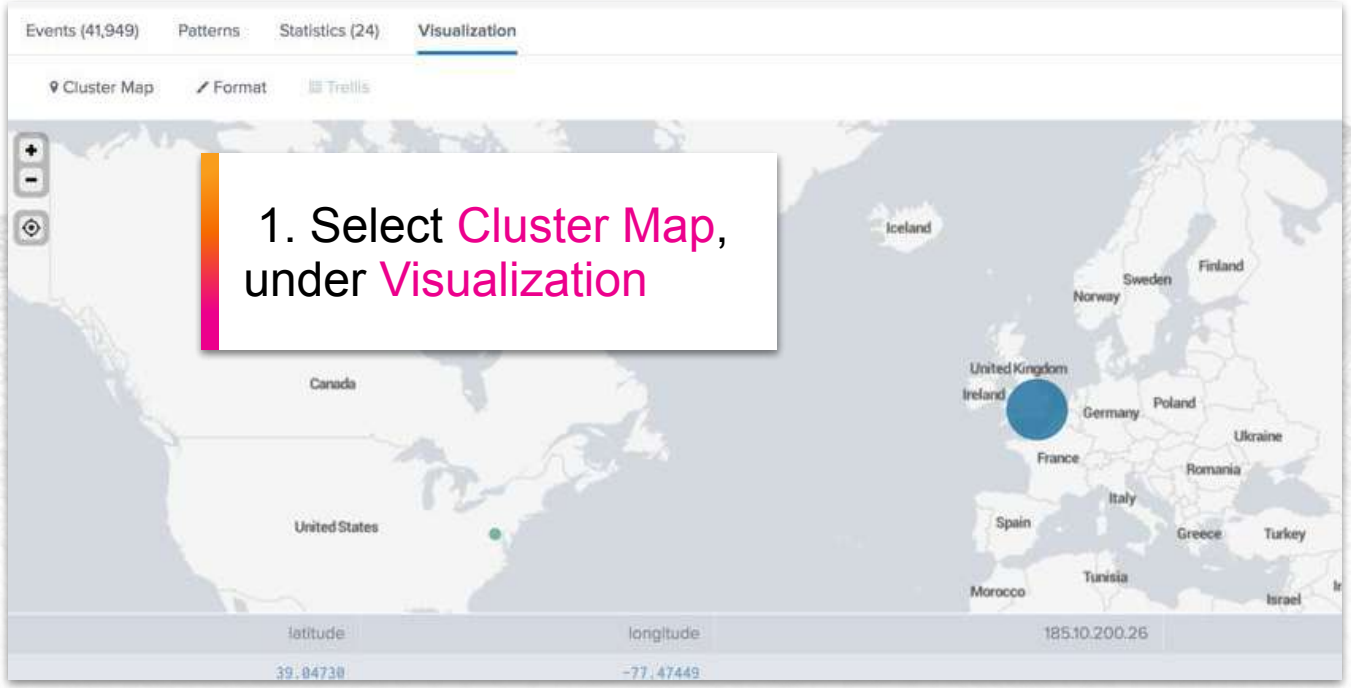

```
tag=authentication NOT src_ip=192.168.0.0/16 | iplocation src_ip
| geostats latfield=lat longfield=lon count by src_ip
```

splunk>

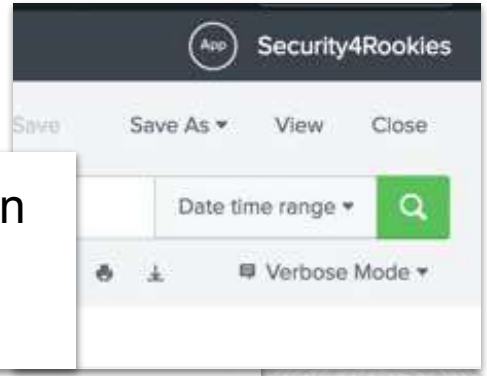
Dashboards

Chpt 6 - Search 2

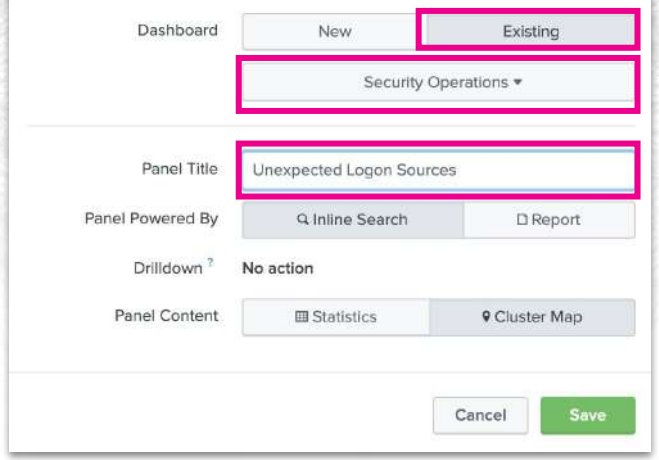
Unexpected Logon Sources



1. Select Cluster Map, under Visualization



2. Click Save As, Then add to Existing, and select your dashboard



splunk>

Dashboards

Chpt 6 - Search 3

Analyse Useragent Lengths

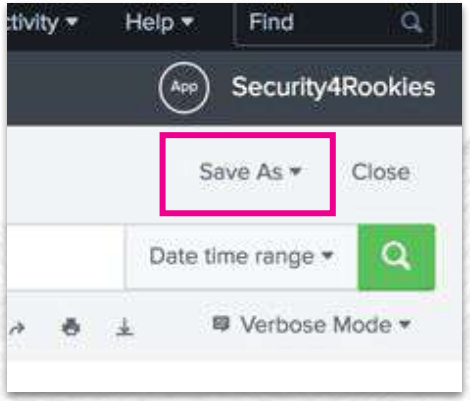

```
index=botsv1 sourcetype=stream:http | eval ua_len=len(http_user_agent)
| stats count values(ua_len) AS ua_len by http_user_agent | sort ua_len, count
```

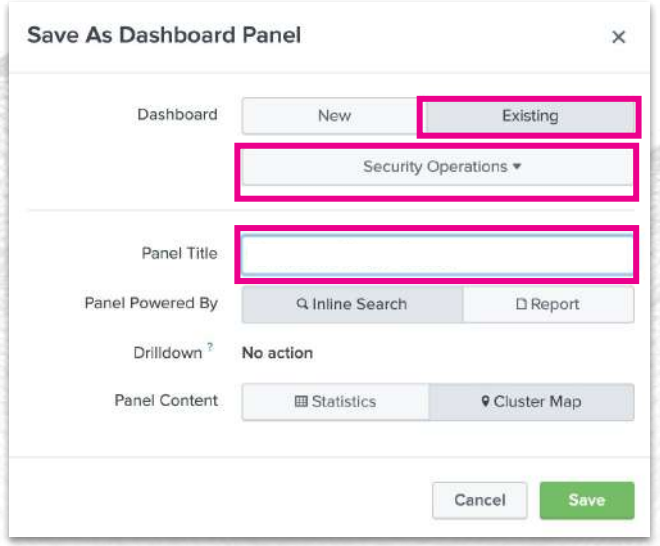
splunk>

Dashboards

Chpt 6 - Search 3

Analyse Useragent Lengths





splunk>

Dashboards

Chpt 6 - Search 4

Analyse Web Traffic

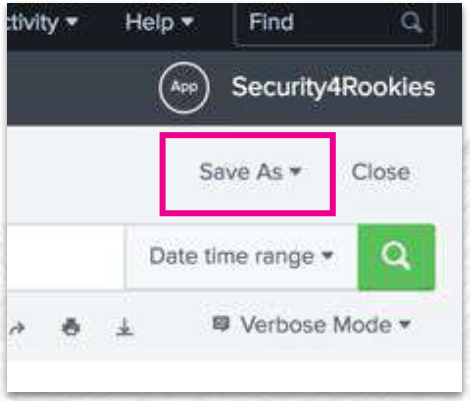

```
index="botsv1" sourcetype=stream:http dest_ip=192.168.250.70
| timechart count BY http_method
```

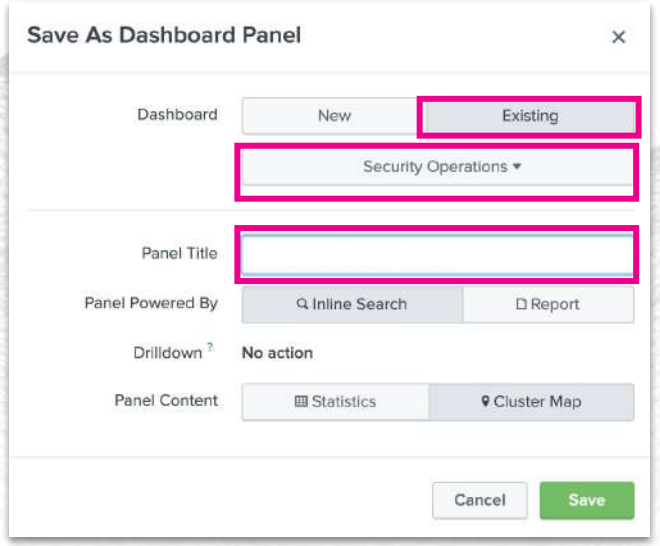
splunk>

Dashboards

Chpt 6 - Search 4

Analyse Web Traffic





splunk>

Dashboards

Chpt 6 - Search 5

Web Logins by External IP

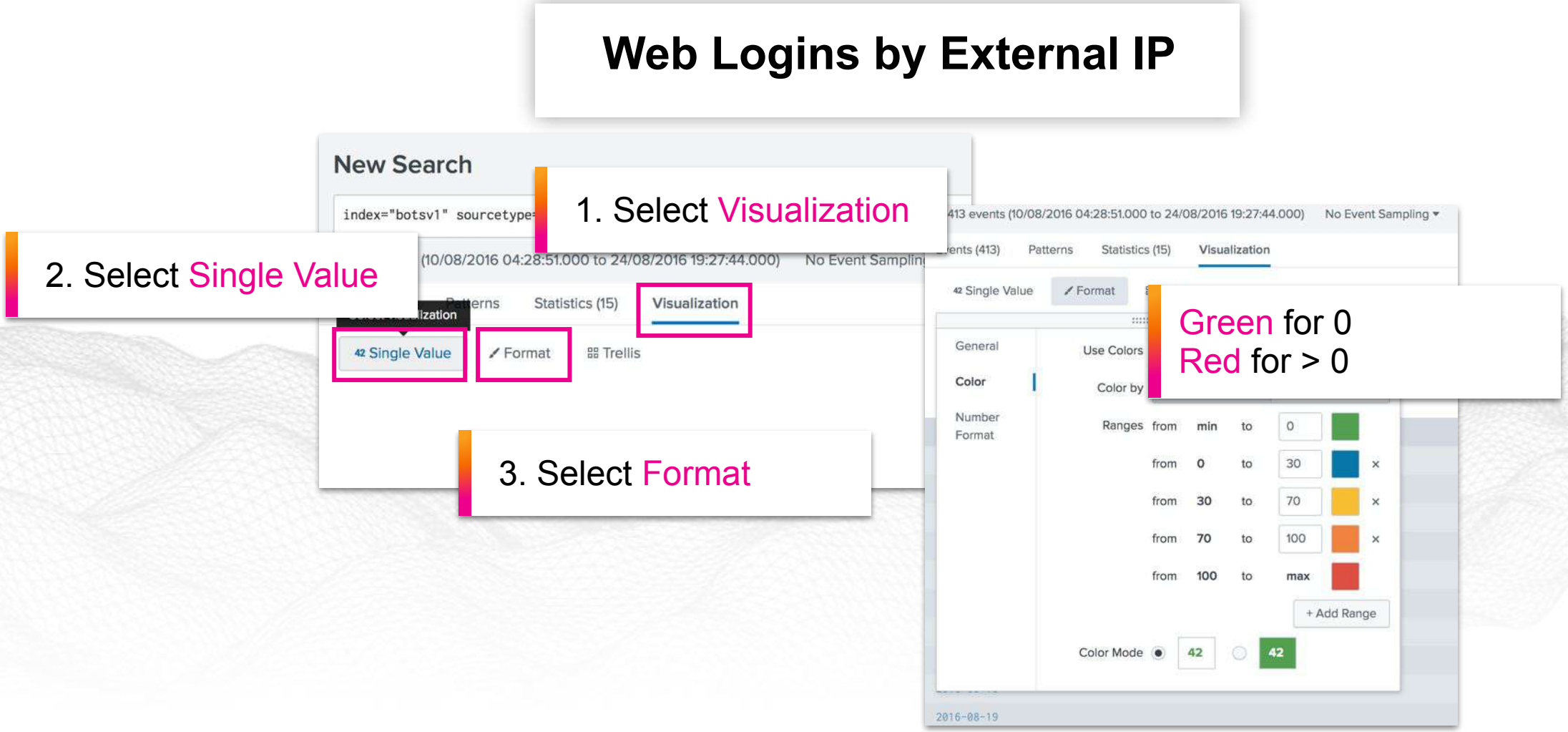

```
index="botsv1" sourcetype=stream:http dest_ip=192.168.250.70
src_ip!="192.168.0.0/16" http_method=post form_data=*username*passwd*
| timechart count
```

splunk>

Dashboards

Chpt 6 - Search 5

Web Logins by External IP

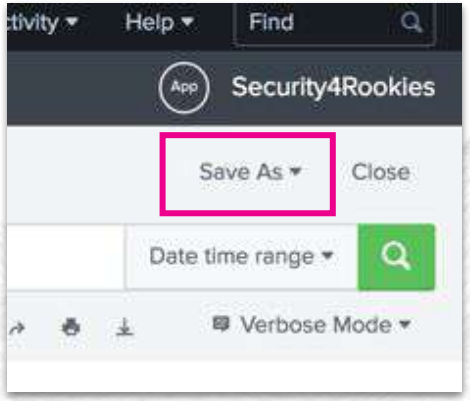


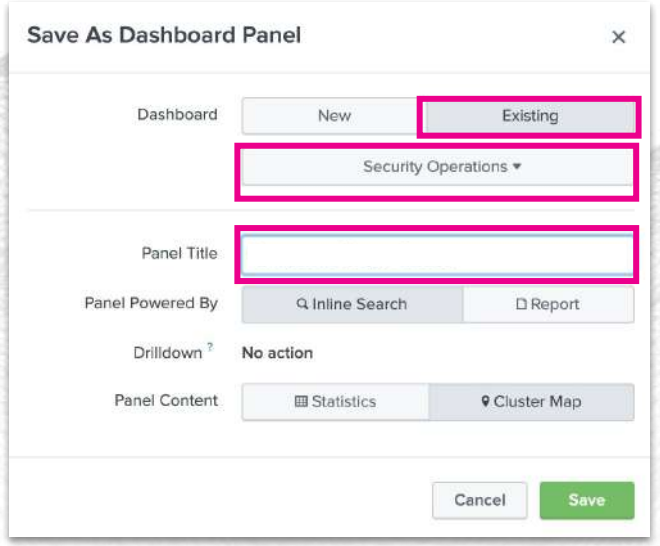
splunk>

Dashboards

Chpt 6 - Search 5

Web Logins by External IP





splunk>

Dashboards

Chpt 6 - Search 6

Scanning Activity

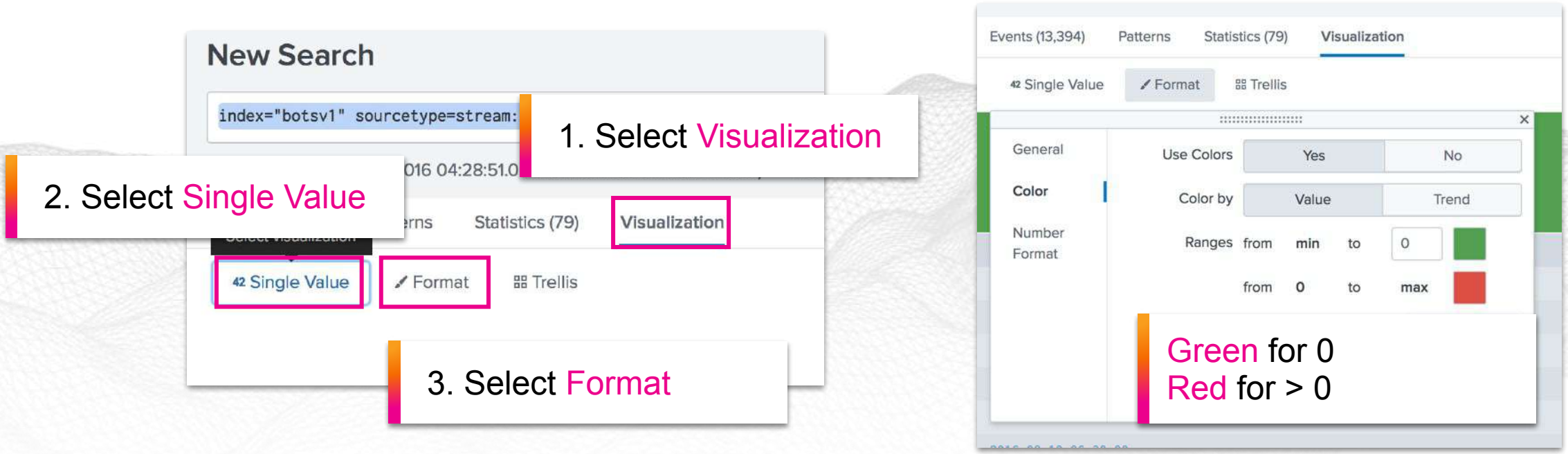

```
index="botsv1" sourcetype=stream:http dest_ip=192.168.250.70 src_headers="*acunetix*"
| timechart count
```

splunk>

Dashboards

Chpt 6 - Search 6

Scanning Activity

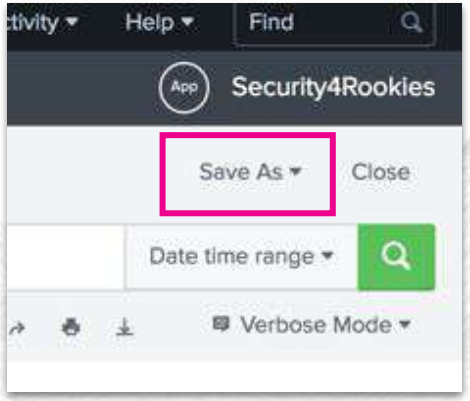


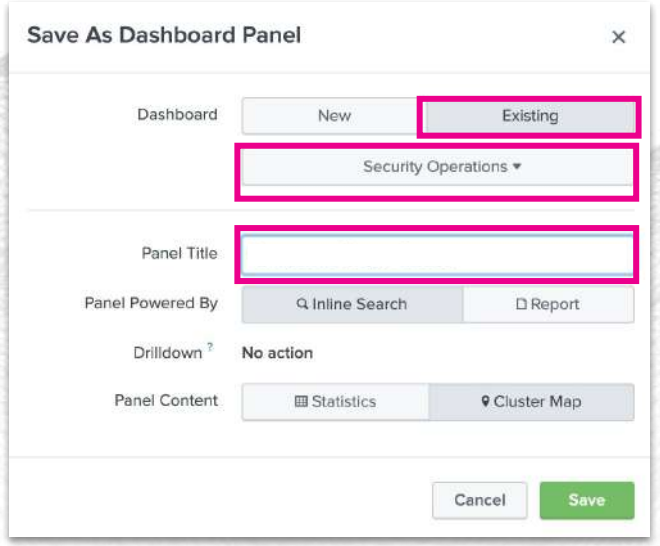
splunk>

Dashboards

Chpt 6 - Search 6

Scanning Activity

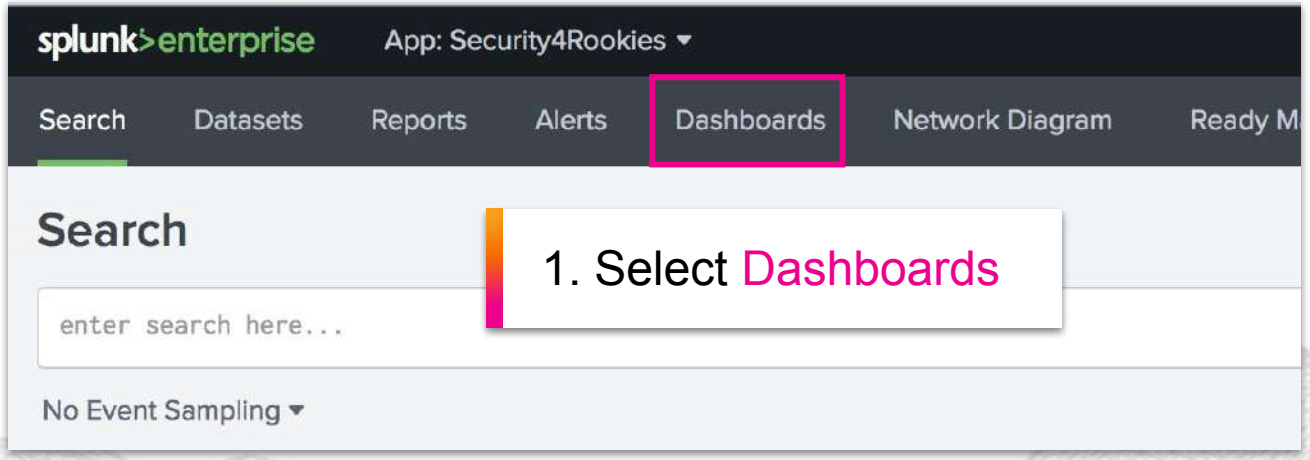




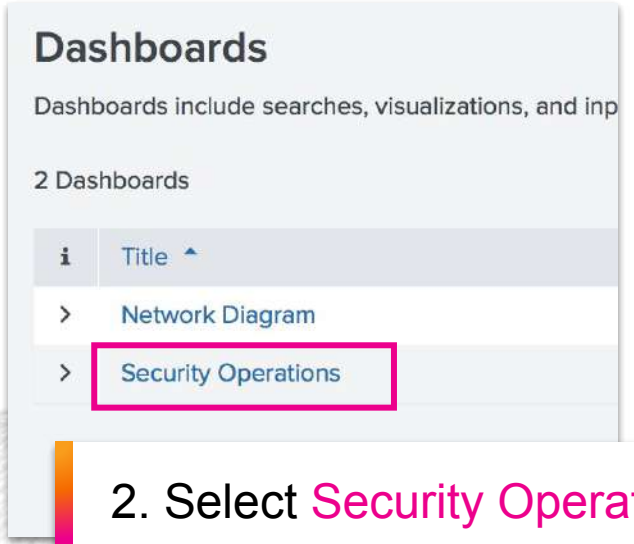
splunk>

Dashboards

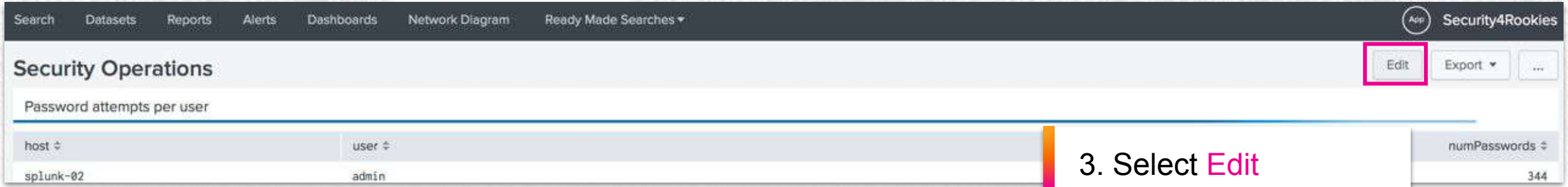
Select Dashboard



1. Select Dashboards



2. Select Security Operations

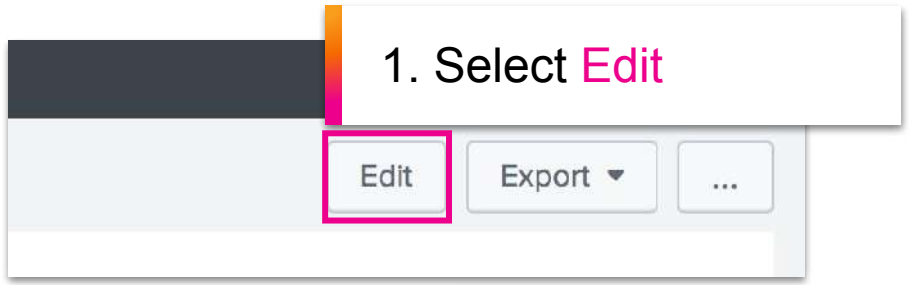


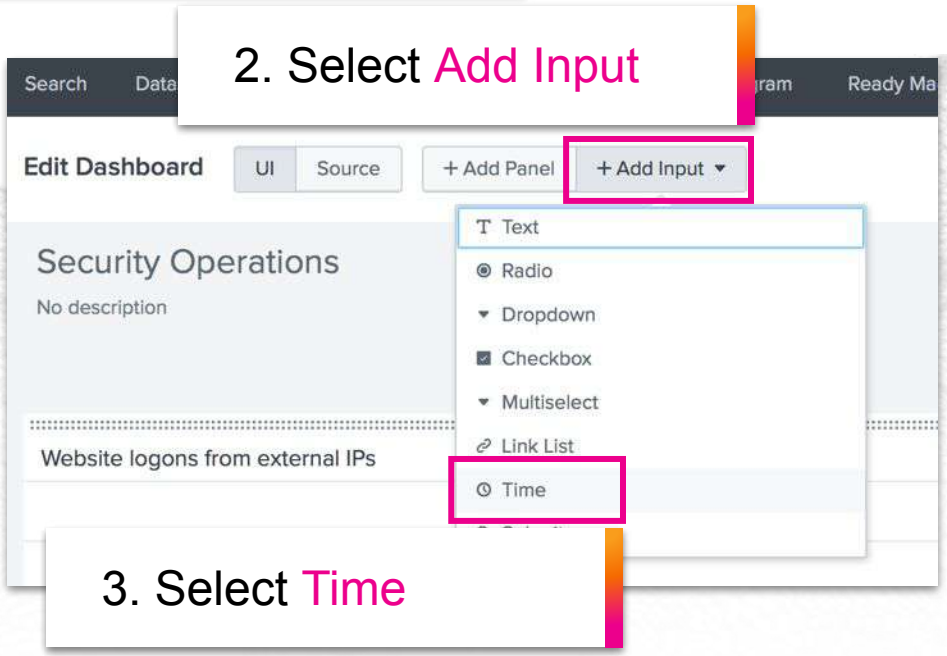
3. Select Edit

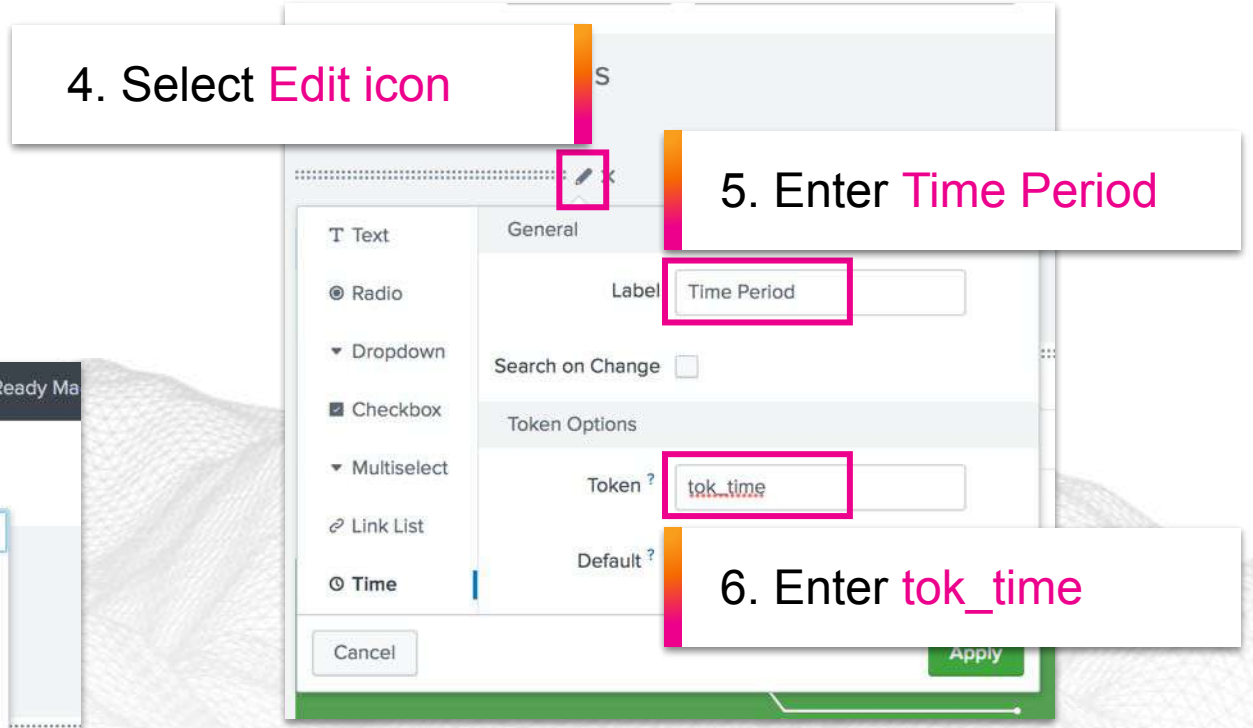
splunk>

Dashboards

Add Input



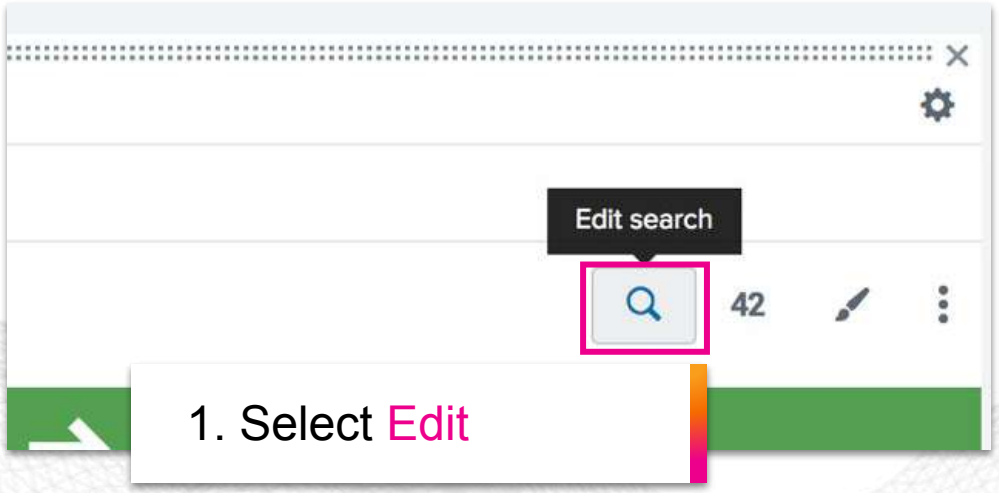




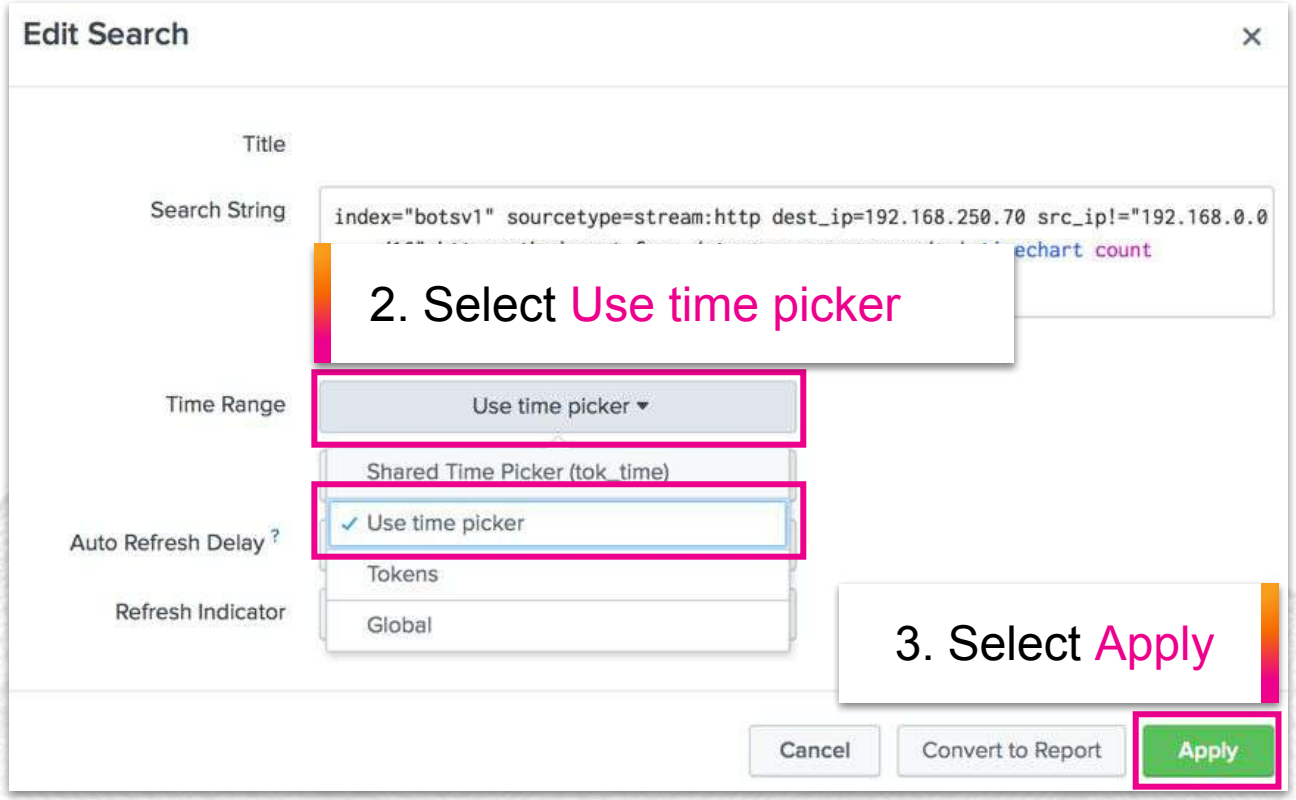
splunk>

Dashboards

Use Token



1. Select Edit



2. Select Use time picker

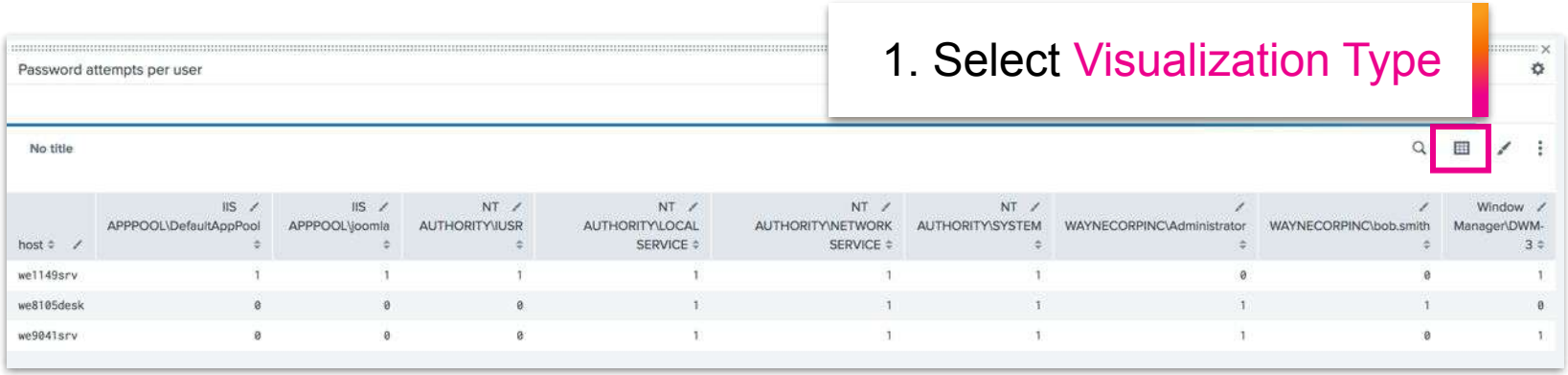
3. Select Apply

4. Repeat for all panels

splunk>

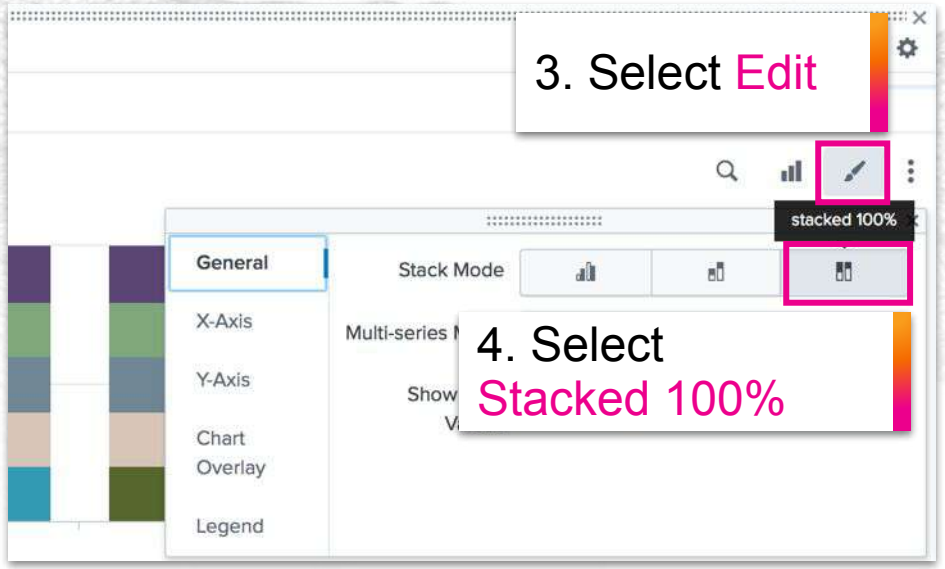
Dashboards

Change Visualisation



1. Select Visualization Type

2. Select Column Chart



3. Select Edit

4. Select Stacked 100%

splunk>

Dashboards

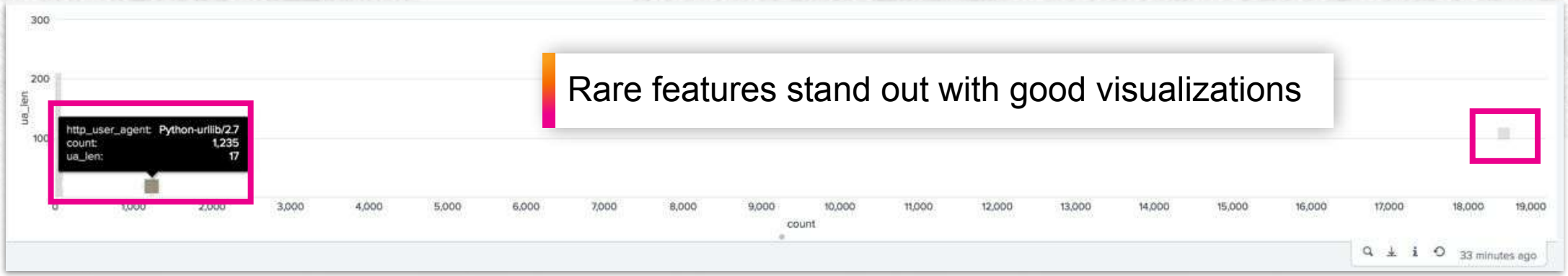
Visualizations

Bonus Challenge: Change http_user_agent panel to a scatter chart

http_user_agent	count	ua_len
)	1	
\	1	
'"	1	
1''	1	
1 ⍰⍰	1	
<!--	1	
JyI=	1	4
⍰'⍰"	1	4
MSDW	2	4
⍰''⍰""	1	6

« prev 1 2 3 4 5 6 7 8 9 10 next »

Wrong type of visual for the data!



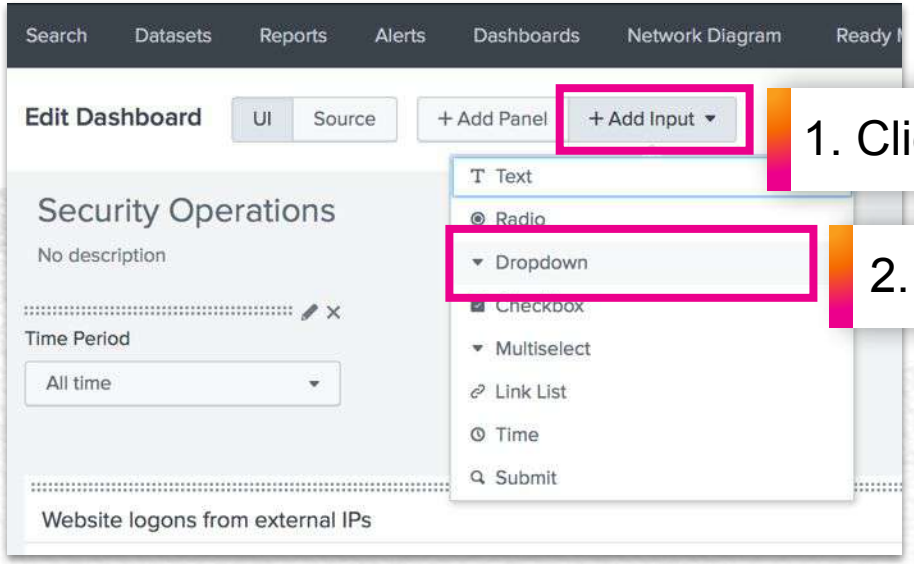
Rare features stand out with good visualizations

splunk>

Dashboards

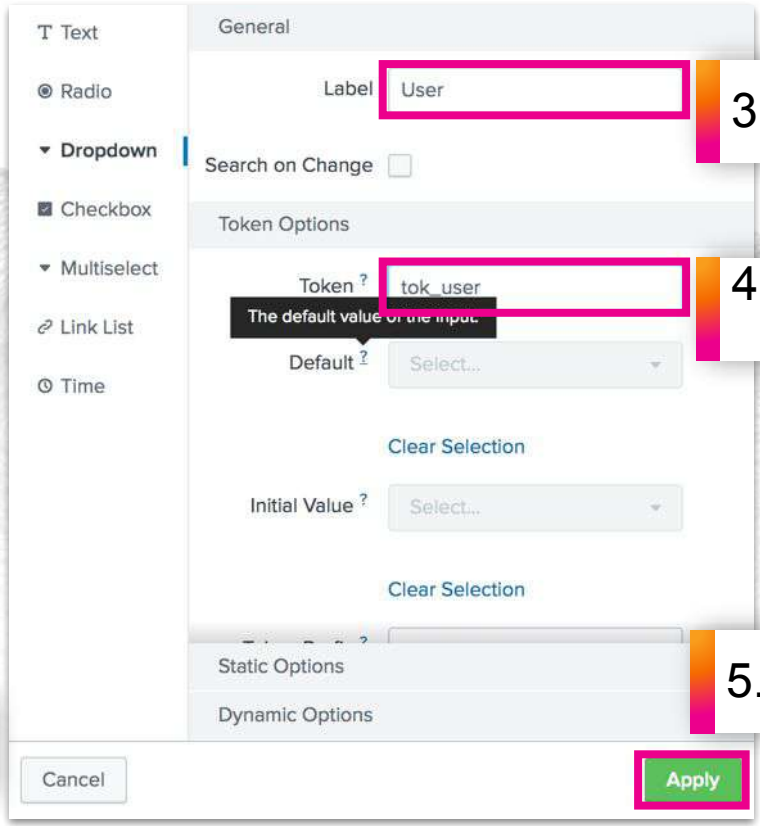
Visualizations

Interactive Filtering



1. Click Add Input

2. Select Dropdown



3. Enter user

4. Enter tok_user

5. Click Apply

6. Scroll down

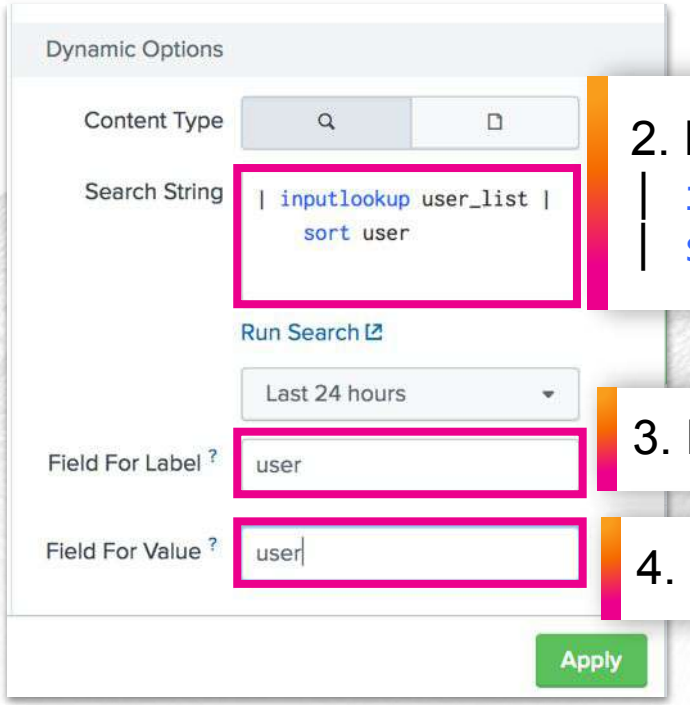
splunk>

Dashboards

Visualizations

Interactive Filtering

1. Enter ALL for Name and * for Value



2. Enter
```
| inputlookup user_list
| sort user
```

3. Enter user

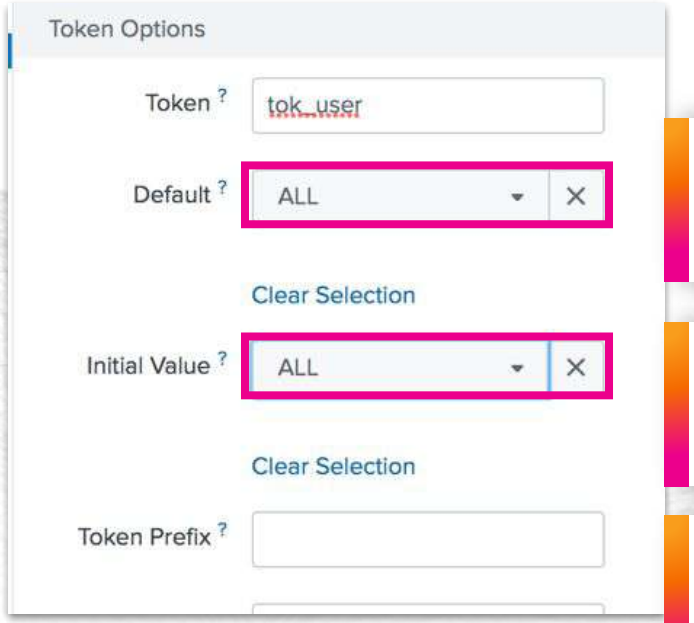
4. Enter user

splunk>

Dashboards

Visualizations

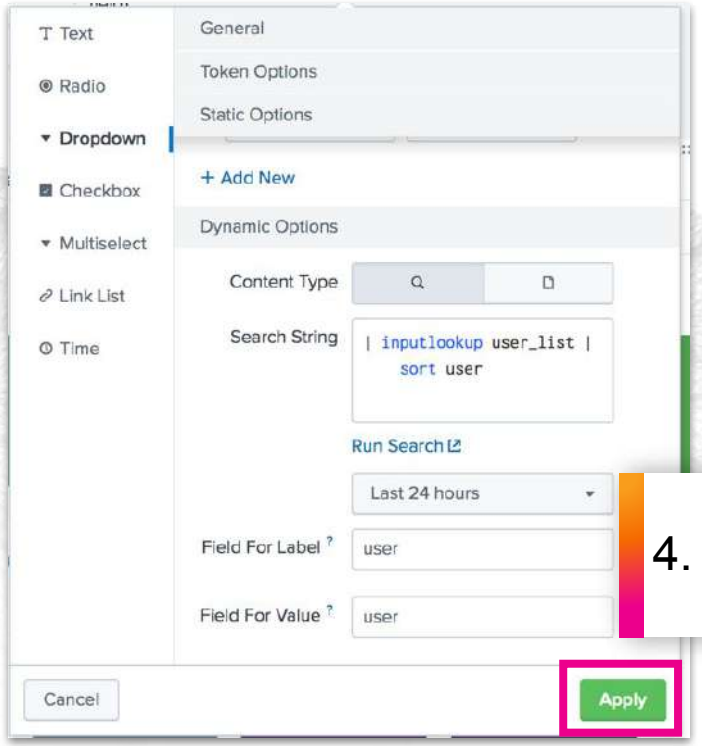
Interactive Filtering



1. Select ALL

2. Select ALL

3. Scroll back up



4. Click Apply

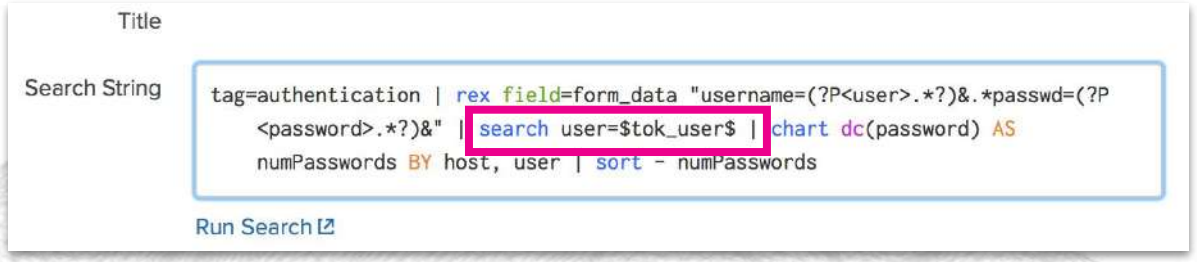
splunk>

Dashboards

Visualizations

Substitute tokens into a dashboard search

1. Click the Magnifying Glass



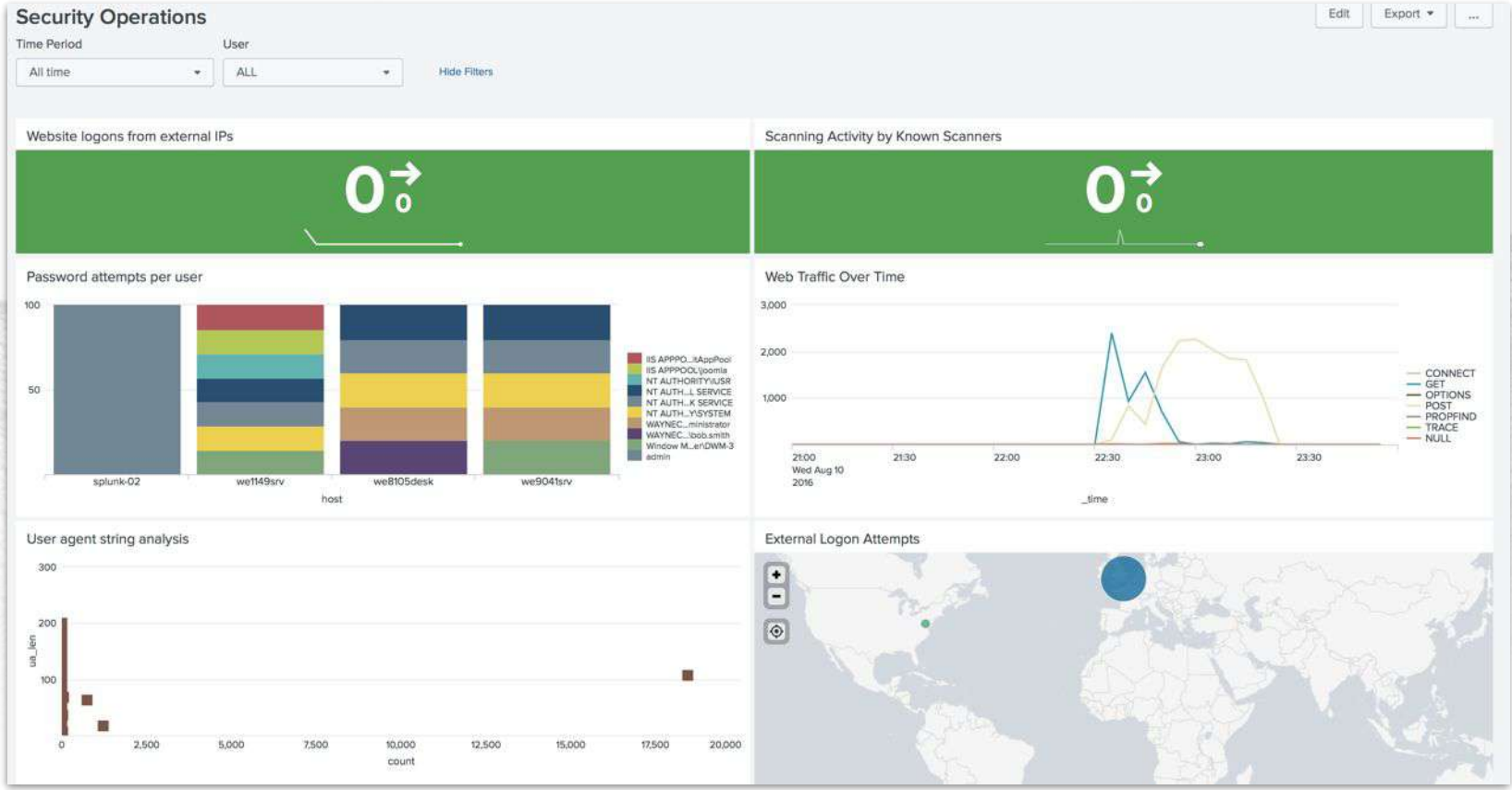
2. Add
   `search user=$tok_user$ |`

splunk>

Dashboards

Visualizations

Dashboard Complete



Splunk Resources

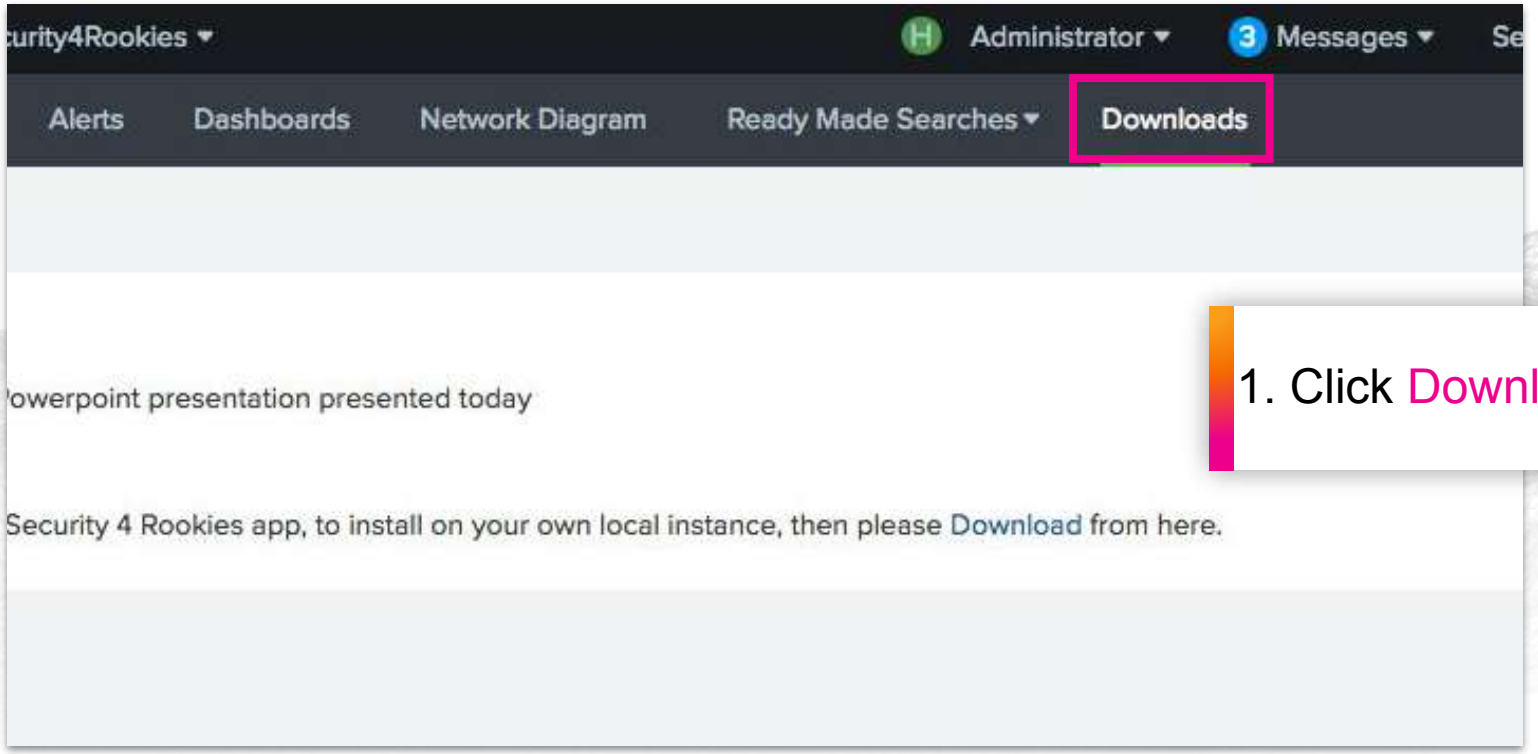
Where to go after today's workshop

splunk>

Dashboards

Visualizations

Dashboard Complete



1. Click Downloads

splunk>

Need more inspiration?

Security Dataset Project

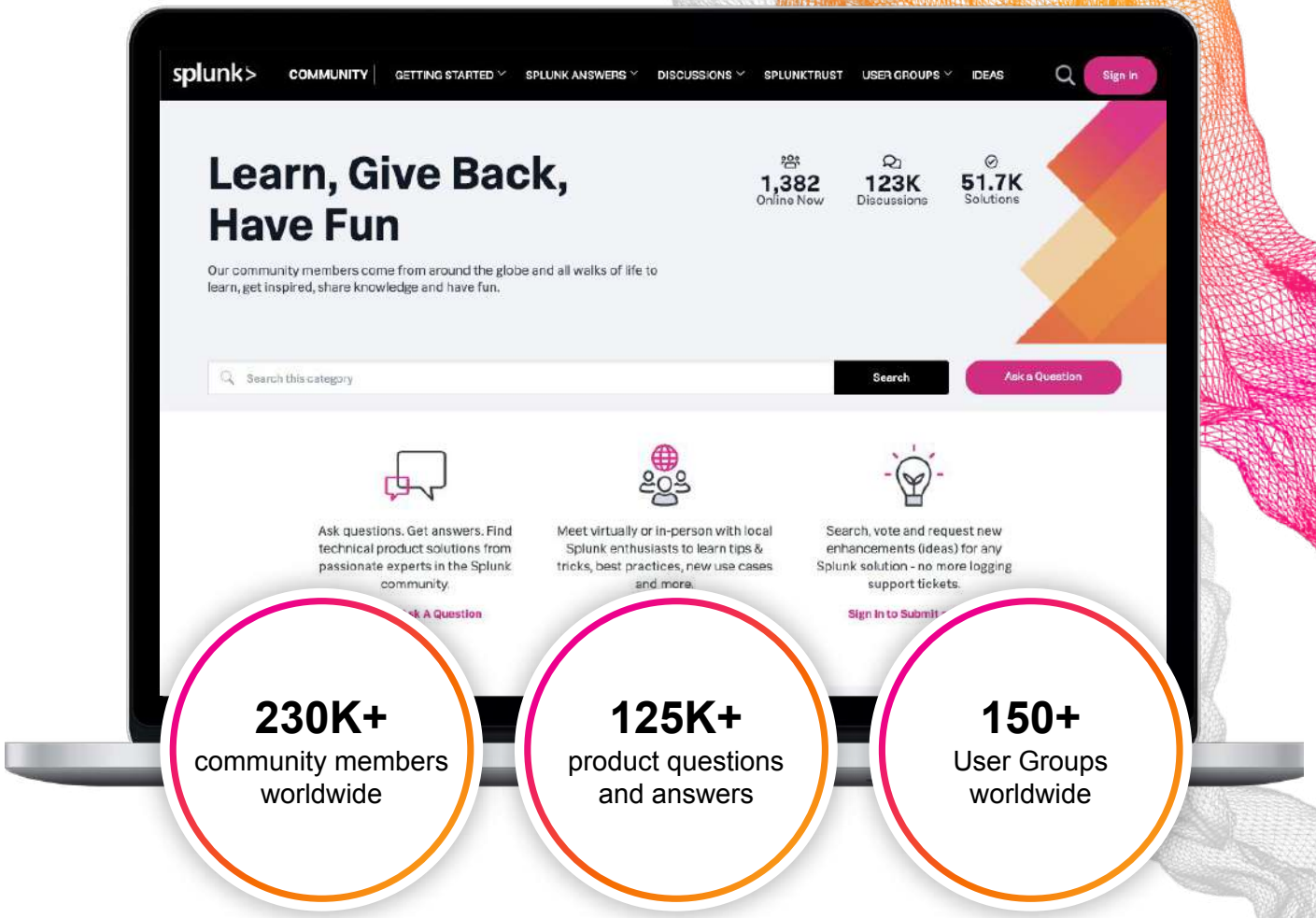
http://live.splunk.com/splunk-security-dataset-project

splunk>

Splunk Community

https://community.splunk.com

- A free way to connect, learn, have fun, and find success with Splunk
- Ask questions, get answers, and find solutions from passionate experts in the community
- Meet in-person or virtually with like-minded enthusiasts, in your area or by interest
- Search for, vote on, or submit your own ideas for new enhancements for any product or solution



splunk>

Splunk Events

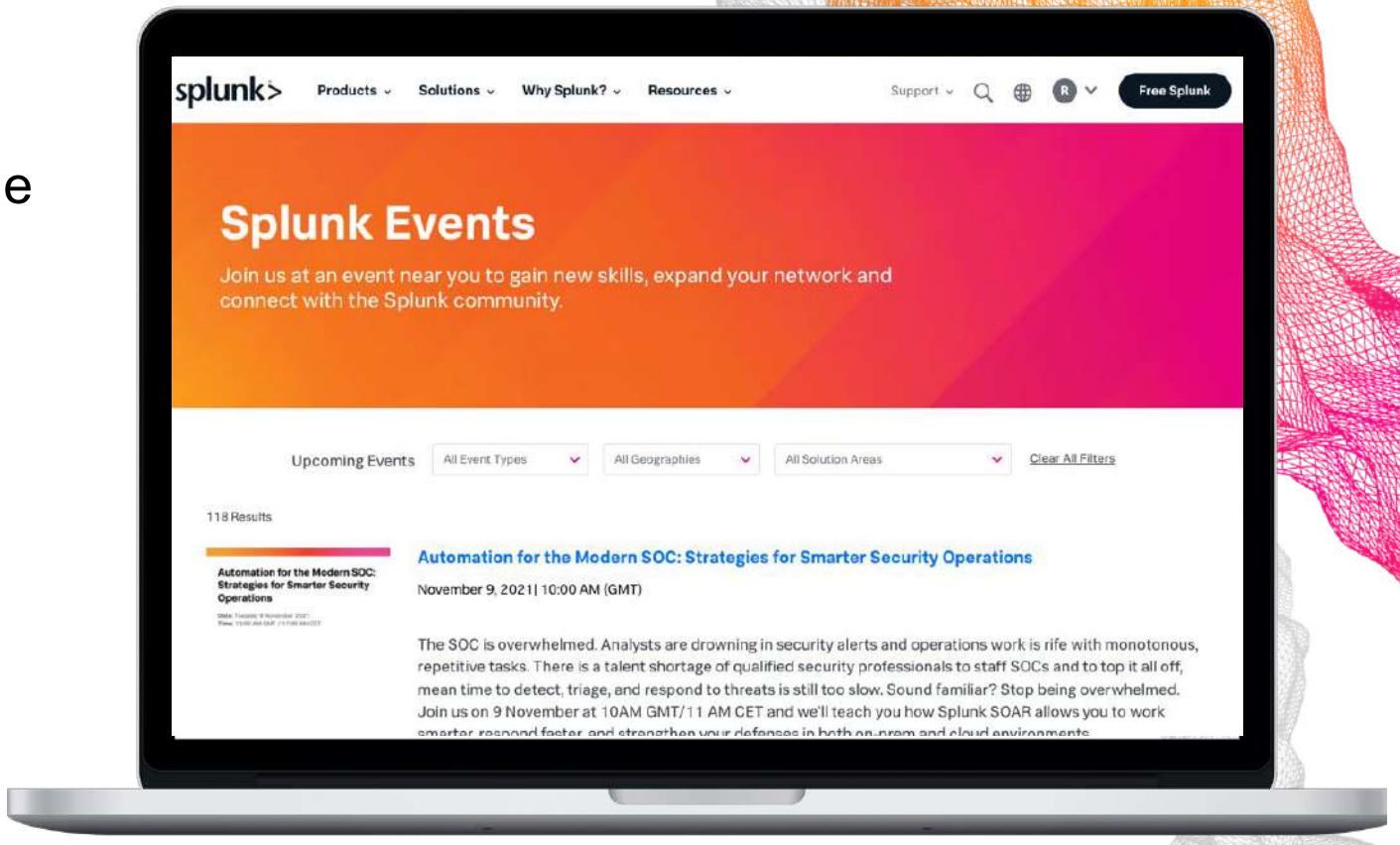
https://events.splunk.com

- Expand your network and connect with the global and local Splunk community

.conf

https://conf.splunk.com

- Join us at .conf23!
- Hundreds of on-demand sessions from product updates to learning new Splunk skills!

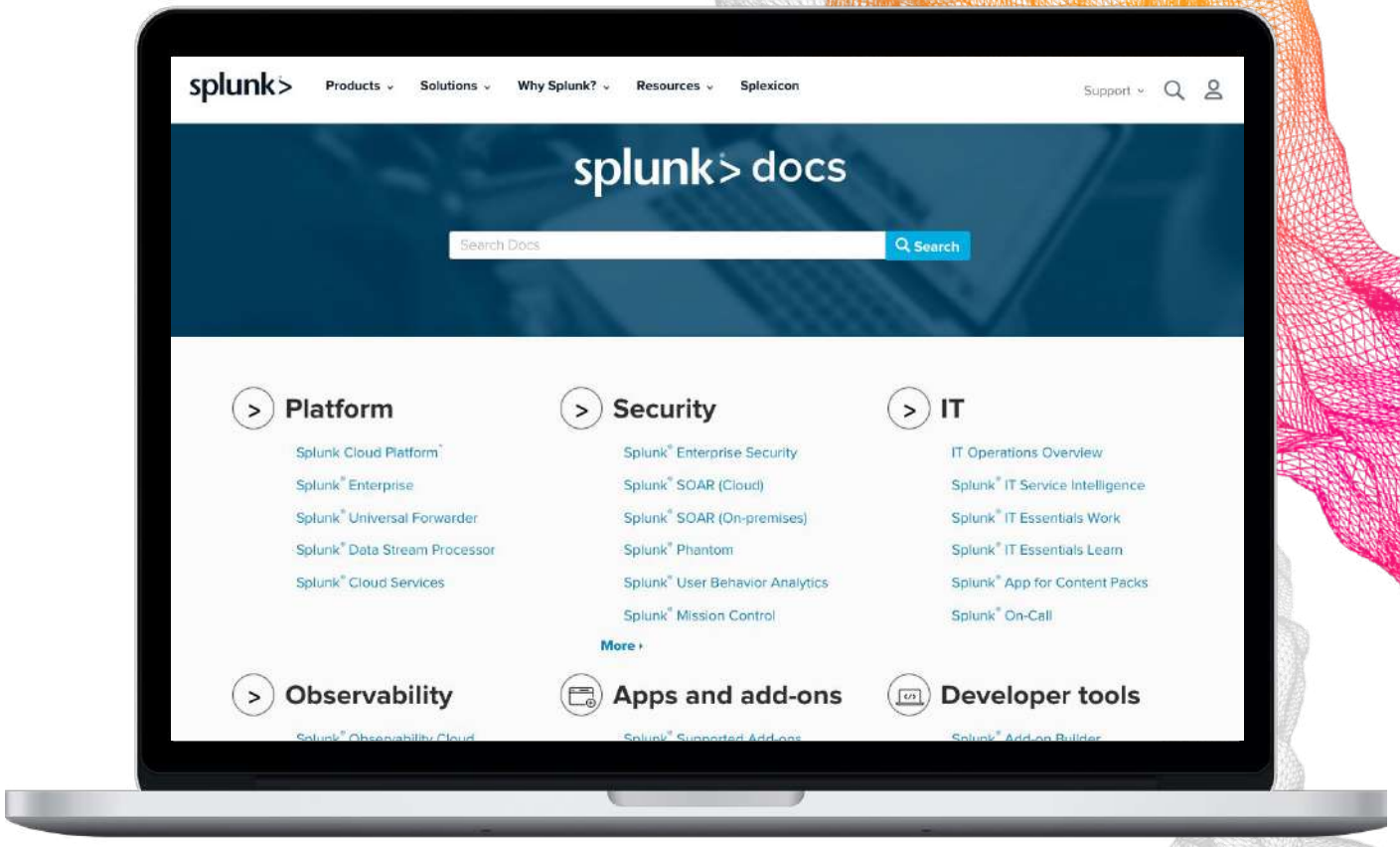


splunk>

Documentation

https://docs.splunk.com

- Search reference for SPL
- Step-by-step tutorials
  Search
  https://splk.it/SplunkSearchTutorial
  Dashboard Studio
  https://splk.it/SplunkDashStudioTutorial
- Product references
- Procedures/guides
- And more!

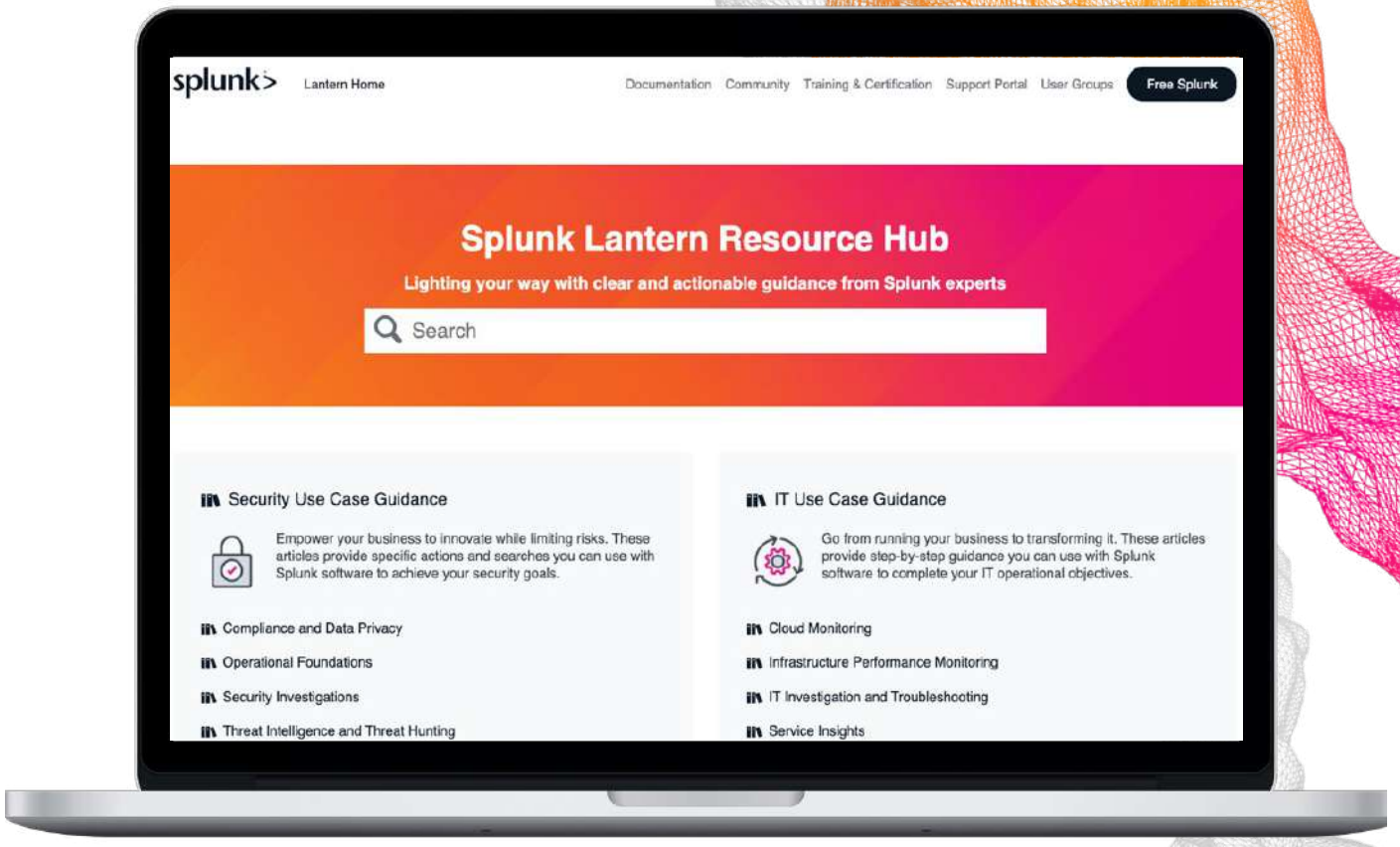


splunk>

Splunk Lantern

https://lantern.splunk.com

- Use case library
- Step-by-step procedures
- Map use cases to data sources
- Splunk Success Framework to realize value across your organisation

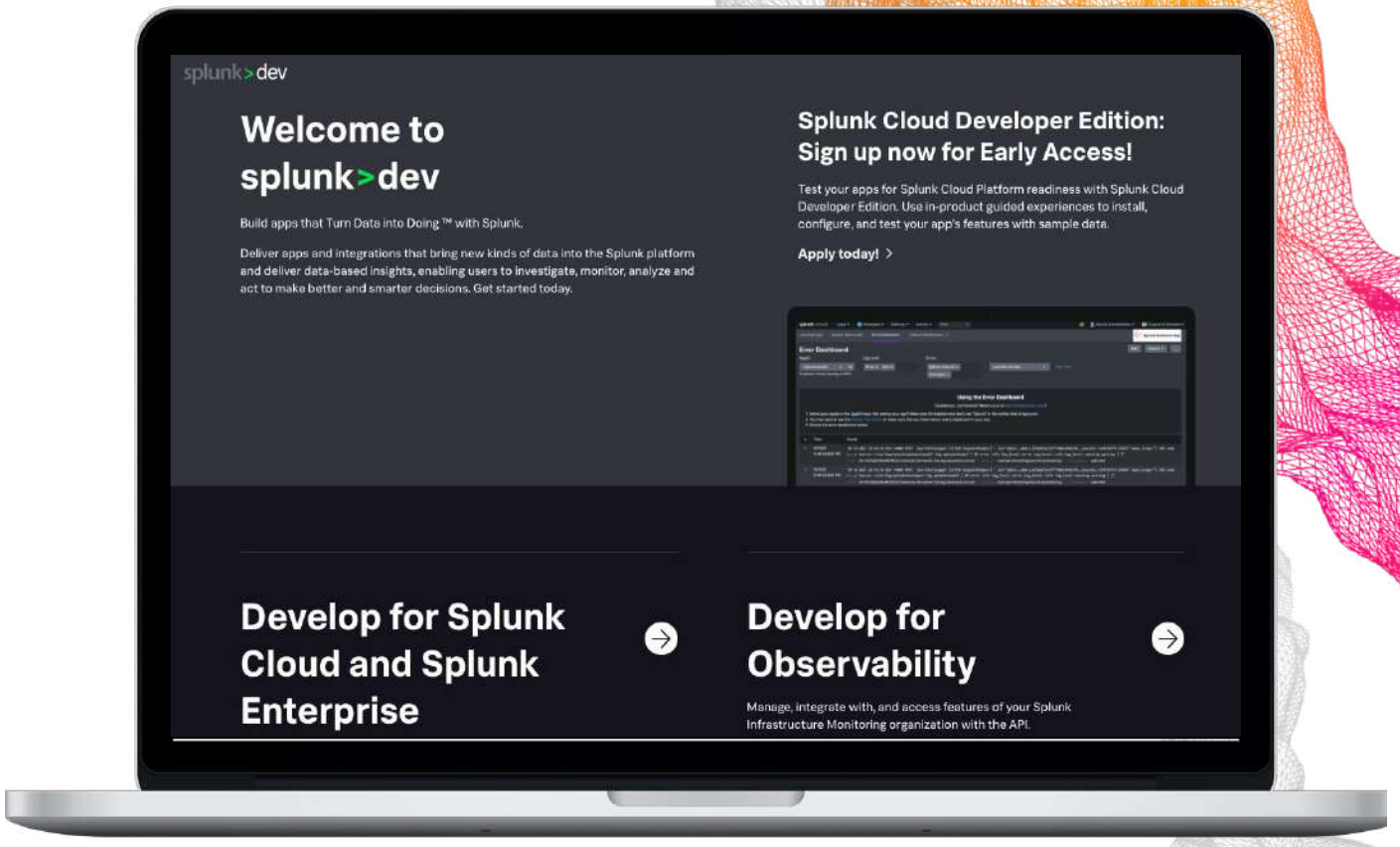


splunk>

Developer Resources

https://dev.splunk.com

- Developer Guide
- API Reference
- Tutorials
- Downloads
  APIs, libraries, tools
- Code examples
- Free Developer licence
- Splunk Cloud Developer Edition
  Test your apps for Splunk Cloud readiness

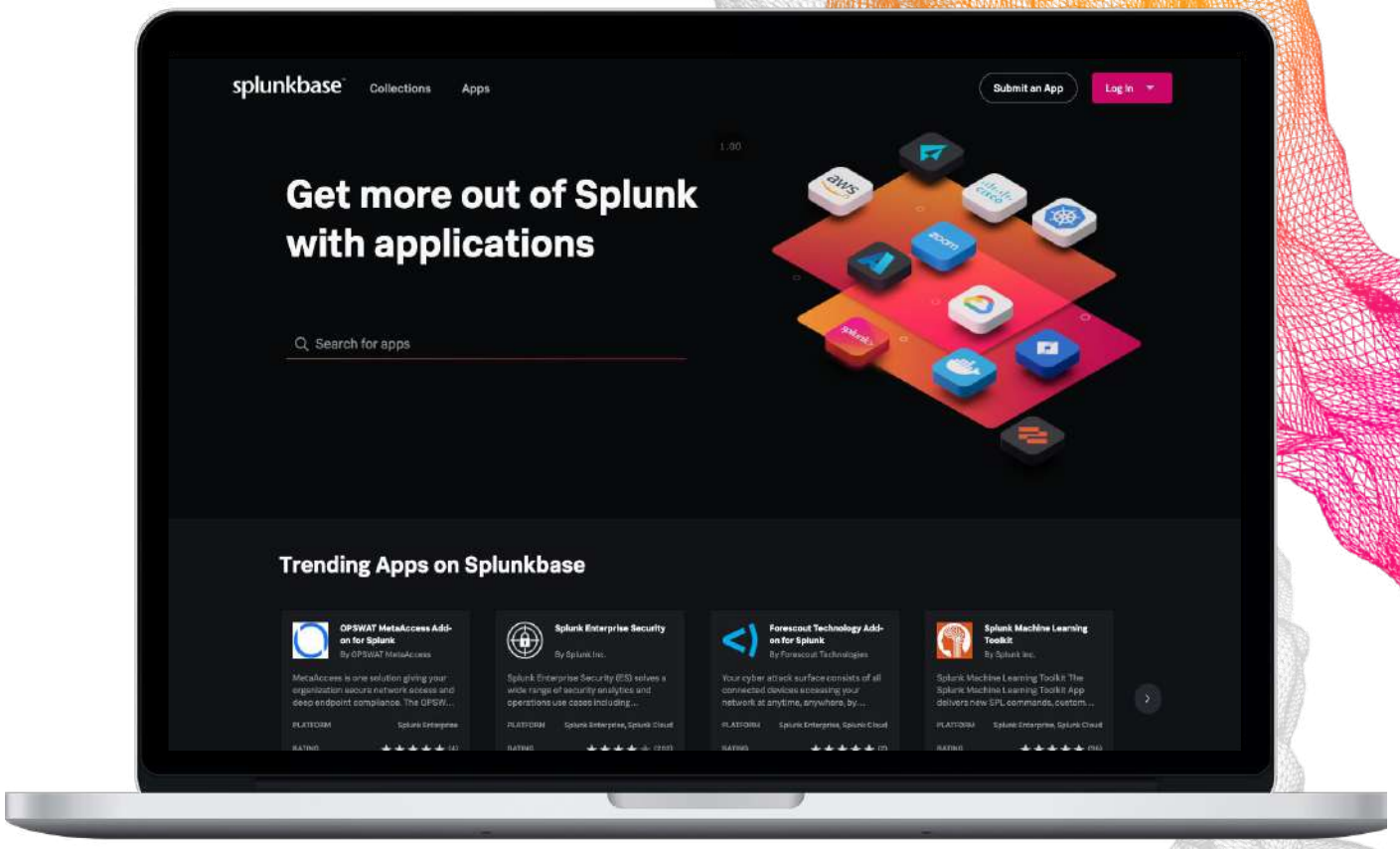


splunk>

Splunk Apps & Add-ons

https://splunkbase.splunk.com/

- 2800+ apps and add-ons
- Pre-built searches, reports, visualisations and integrations for specific use cases and technologies
- Download apps and customise them based on your requirements
- Fast time to value from your data
- Build and contribute your own apps!



Training & Certification

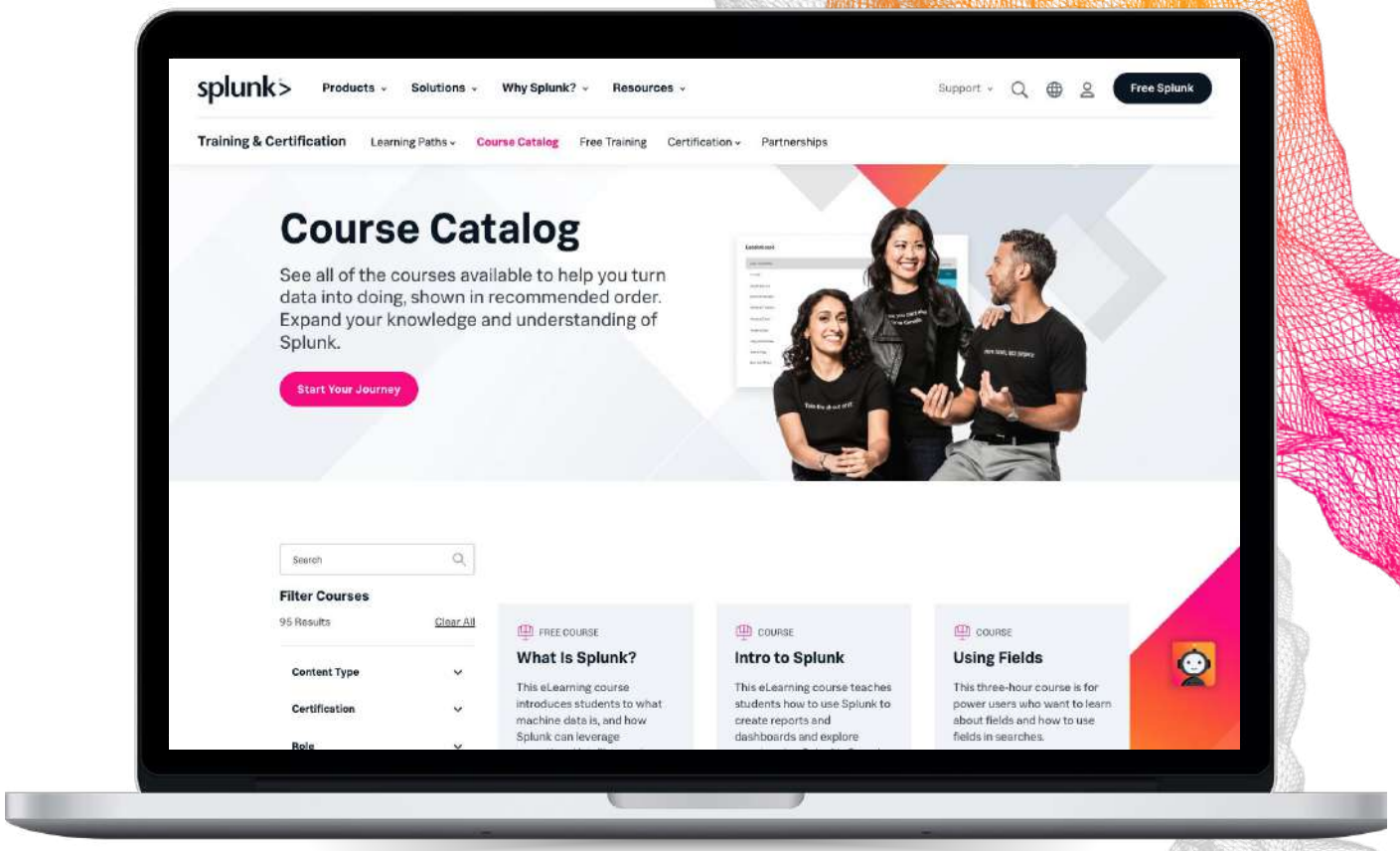
https://splunk.com/training

Online education classes
Instructor-led and self-paced eLearning

Certification tracks for different roles
User, Power User, Admin, Architect and Developer

Splunk Education Rewards
Complete training and receive points that you can redeem for Splunk swag!

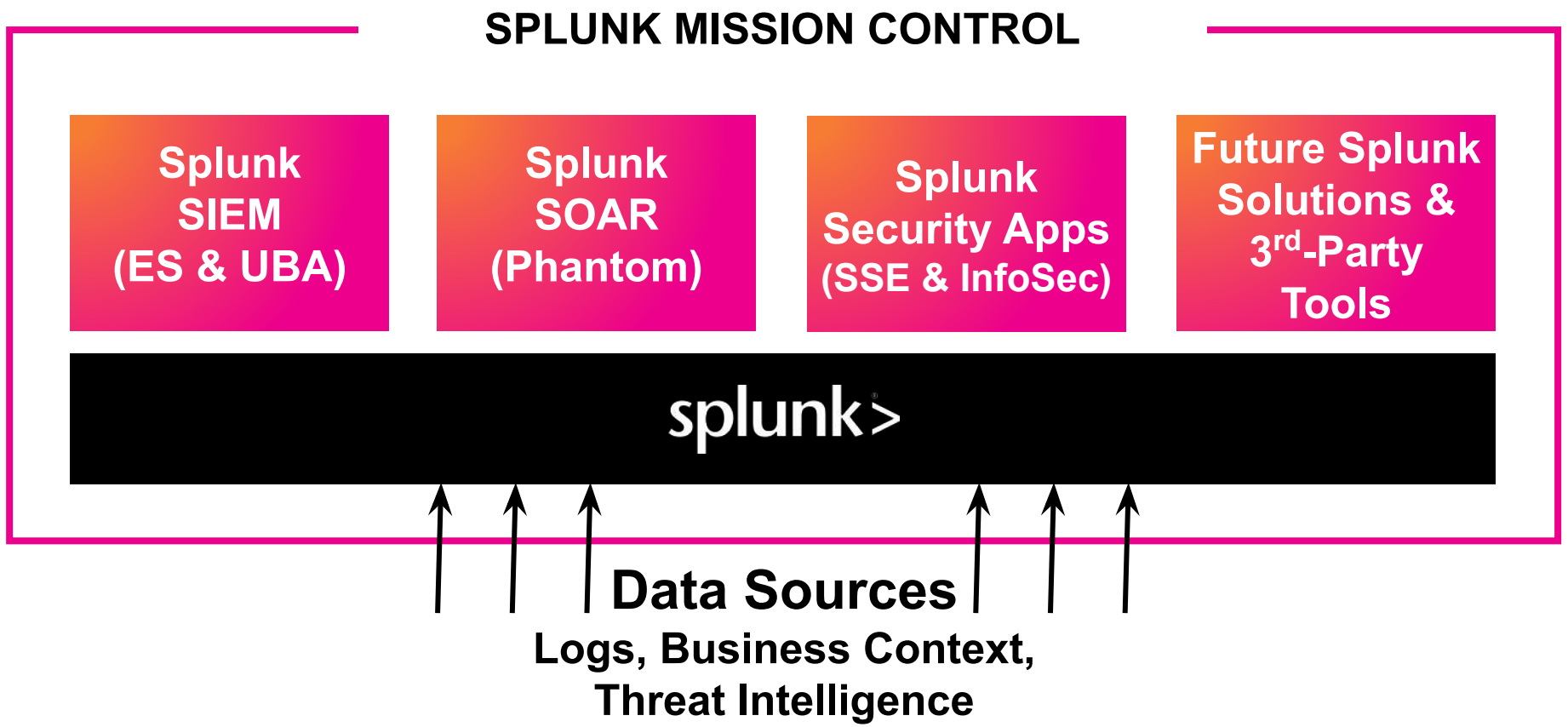
Free education!
Free single-subject eLearning courses to kick start your Splunk learning



splunk>

Splunk for Security

Unifying **data**, **analytics**, and **operations**



Thank You!