1. Register the lab environment:
https://splunk4rookies.com/10411/self_register

Splunk Security 4 Rookies

Daniel Yeung, Partner Technical Manager | Splunk

2. Download the presentation deck:
https://drive.google.com/drive/folders/1wLkH44jjVWhKfy5F8yUhSJ78H7Z2FVb4?usp=share_link

splunk> turn data into doing™

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. 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. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Agenda for Today's Workshop

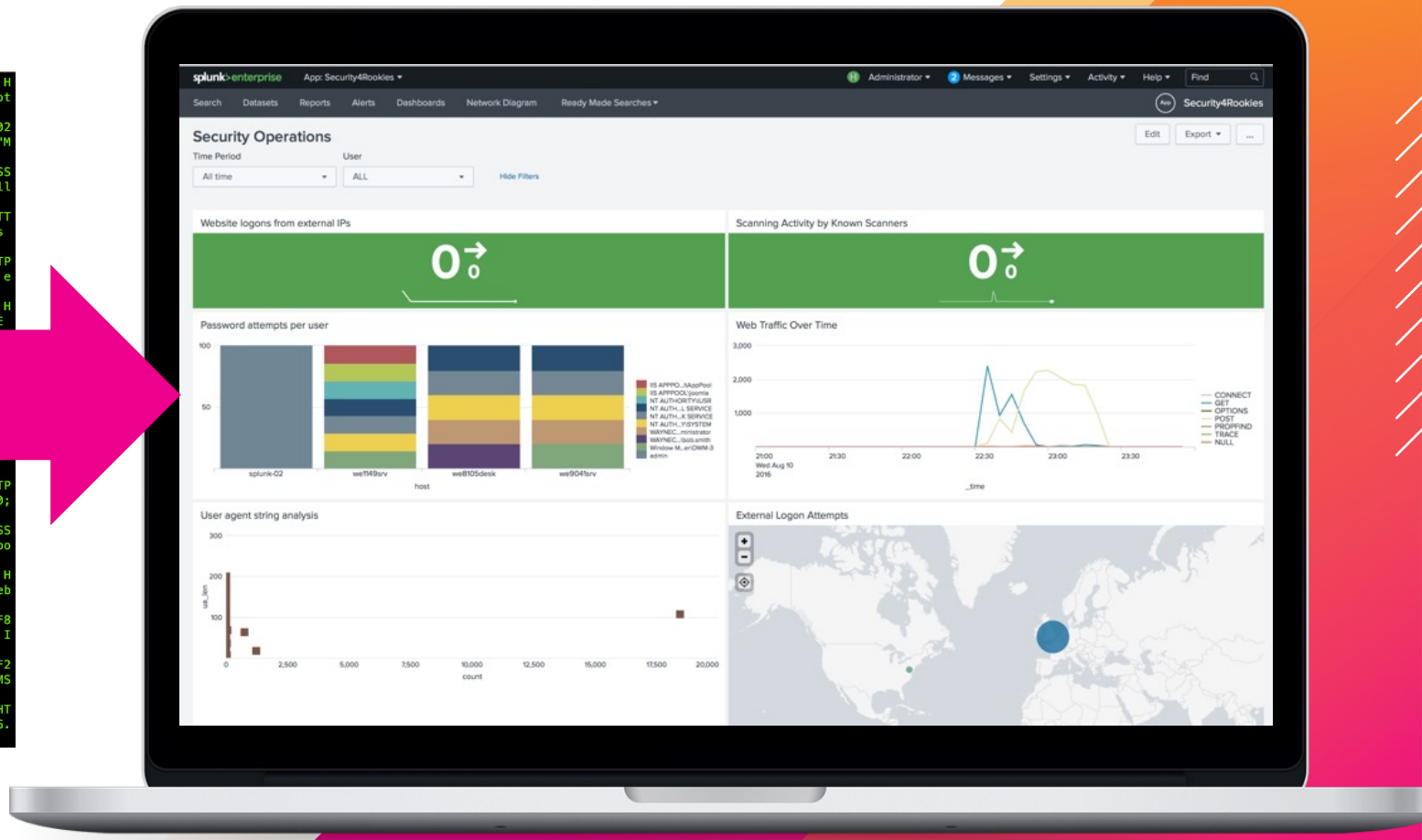
- ✓ Brief Splunk overview
- ✓ Search basics
- ✓ Indexing data
- ✓ Defining the format of your data
- ✓ Making data useable
- ✓ Aggregating and correlating data
- ✓ Put it into practice on web defacement investigation
- ✓ Creating proactive searches and dashboards

There's a Lot More to Splunk…

- Clustering
- Data Models
- Alerting
- Pivot
- Data Tables
- SDKs
- APIs
- DB Connect
- Splunk Stream
- Deployment Server
- Replication
- Data Stream Processor
- Data Fabric Search
- Metrics
- Advanced Searches
- Machine Learning (ML)
- Custom Visualisations
- HTTP Event Collector (HEC)
- Data Filtering
- Transformations
- Architecture
- Report Acceleration
- Common Information Model (CIM)
- Containers
- Best Practices
- And much more...

Objective

```
9.167.143.32 - - [01/Nov/2016 20:48:22:143] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL1FF4ADFF3 H
TTP 1.1" 200 1429 "http://www.myflowershop.com/cart.do?action=remove&itemId=EST-13&product_id=AV-CB-01" "Googlebot
/2.1 ( http://www.googlebot.com/bot.html) " 403
194.215.205.19 - - [01/Nov/2016 20:48:24:159] "GET /cart.do?action=changequantity&itemId=EST-7&product_id=FI-FW-02
&JSESSIONID=SD1SL2FF9ADFF9 HTTP 1.1" 503 3699 "http://www.myflowershop.com/category.screen?category_id=FLOWERS" "M
ozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 301
130.253.37.97 - - [01/Nov/2016 20:48:24:198] "GET /cart.do?action=purchase&itemId=EST-27&product_id=RP-SN-01&JSESS
IONID=SD3SL8FF4ADFF8 HTTP 1.1" 200 3350 "http://www.myflowershop.com/category.screen?category_id=SURPRISE" "Mozill
a/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 927
92.1.170.135 - - [01/Nov/2016 20:48:25:142] "GET /category.screen?category_id=TEDDY&JSESSIONID=SD1SL1FF10ADFF5 HTT
P 1.1" 200 2906 "http://www.myflowershop.com/category.screen?category_id=TEDDY" "Mozilla/5.0 (Windows; U; Windows
NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6" 967
27.101.0.0 - - [01/Nov/2016 20:48:25:130] "GET /product.screen?product_id=FL-DLH-02&JSESSIONID=SD1SL6FF1ADFF6 HTTP
 1.1" 200 3994 "http://www.myflowershop.com/product.screen?product_id=FL-DLH-02" "Opera/9.01 (Windows NT 5.1; U; e
n)" 389
125.17.14.100 - - [01/Nov/2016 20:48:26:174] "GET /product.screen?product_id=AV-CB-01&JSESSIONID=SD3SL10FF4ADFF2 H
TTP 1.1" 503 2474 "http://www.myflowershop.com/product.screen?product_id=AV-CB-01" "Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1)" 297
128.241.220.82 - - [01/Nov/2016 20:48:28:158] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD3SL10
TTP 1.1" 200 2438 "http://www.myflowershop.com/cart.do?action=view&itemId=EST-18&product_id=FL-DLH-02"
 (Windows NT 6.0; U; en)" 681
131.178.233.243 - - [01/Nov/2016 20:48:30:128] "POST /cart.do?action=purchase&itemId=EST-18&product_id=
ESSIONID=SD3SL1FF9ADFF7 HTTP 1.1" 404 664 "http://www.myflowershop.com/product.screen?product_id=K9-BD-
bot/2.1 ( http://www.googlebot.com/bot.html) " 387
94.229.0.21 - - [01/Nov/2016 20:48:31:177] "GET /category.screen?category_id=BOUQUETS&JSESSIONID=SD4SL7
TTP 1.1" 200 3770 "http://www.myflowershop.com/category.screen?category_id=BOUQUETS" "Mozilla/5.0 (Windows
dows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6" 814
12.130.60.5 - - [01/Nov/2016 20:48:32:150] "GET /product.screen?product_id=AV-CB-01&JSESSIONID=SD1SL4FF5ADFF6 HTTP
 1.1" 200 2676 "http://www.myflowershop.com/category.screen?category_id=TEDDY" "Mozilla/4.0 (compatible; MSIE 6.0;
 Windows NT 5.1)" 177
130.253.37.97 - - [01/Nov/2016 20:48:33:155] "GET /cart.do?action=addtocart&itemId=EST-1&product_id=AV-CB-01&JSESS
IONID=SD10SL9FF9ADFF7 HTTP 1.1" 200 933 "http://www.myflowershop.com/product.screen?product_id=AV-CB-01" "Googlebo
t/2.1 ( http://www.googlebot.com/bot.html) " 493
130.253.37.97 - - [01/Nov/2016 20:48:35:178] "GET /product.screen?product_id=AV-SB-02&JSESSIONID=SD8SL3FF6ADFF10 H
TTP 1.1" 200 3491 "http://www.myflowershop.com/cart.do?action=addtocart&itemId=EST-6&product_id=AV-SB-02" "Googleb
ot/2.1 ( http://www.googlebot.com/bot.html) " 778
131.178.233.243 - - [01/Nov/2016 20:48:35:188] "POST /product.screen?product_id=FI-FW-02&JSESSIONID=SD2SL2FF7ADFF8
 HTTP 1.1" 200 1023 "http://www.myflowershop.com/product.screen?product_id=FI-FW-02" "Mozilla/5.0 (Macintosh; U; I
ntel Mac OS X 10_6_3; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 Safari/533.4" 936
131.178.233.243 - - [01/Nov/2016 20:48:35:172] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD8SL4FF9ADFF2
 HTTP 1.1" 404 3679 "http://www.myflowershop.com/product.screen?product_id=FL-DSH-01" "Mozilla/4.0 (compatible; MS
IE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 402
141.146.8.66 - - [01/Nov/2016 20:48:37:141] "GET /product.screen?product_id=K9-BD-01&JSESSIONID=SD10SL8FF9ADFF8 HT
TP 1.1" 200 1452 "http://www.myflowershop.com/category.screen?category_id=TEDDY" "Mozilla/4.0 (compatible; MSIE 6.
0; Windows NT 5.1)" 118
```



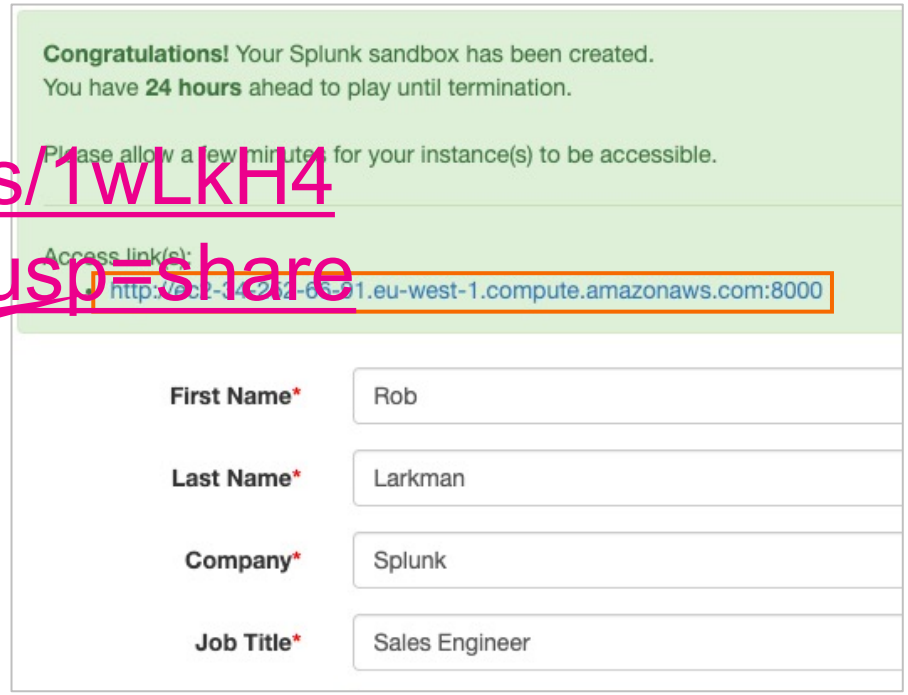
Task 1: Register and Create Your Environment

Tasks:

1. **Register:**
   https://splunk4rookies.com/10411/self_register

2. **Download today's slide deck:**
   https://drive.google.com/drive/folders/1wLkH44jjVWhKfy5F8yUhSJ78H7Z2FVb4?usp=share_link

You will get your own unique link. Your environment will take a few minutes to spin up so please be patient!



splunk> turn data into doing

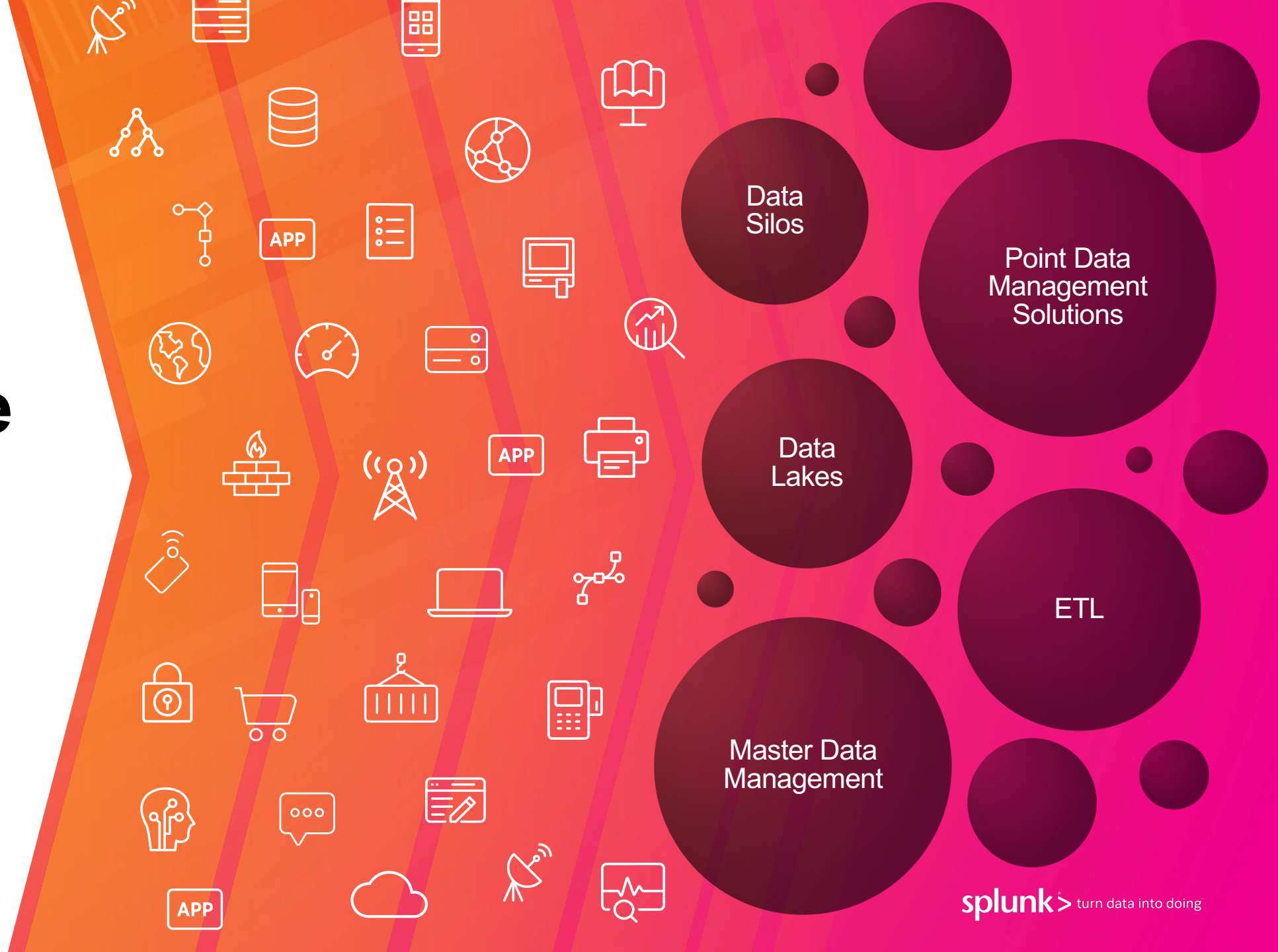
Every Company Has a Universe of Real-time Data

Creating More Opportunities and Threats than Ever Before

- Inventory RFID'S
- Assembly Robots
- Databases
- Business Apps
- Warehouse Utilization Systems
- Control Units
- New Technology
- New Data Streams
- Networks
- New Devices

splunk> turn data into doing

Turning Real-time Data Into Action is Hard



splunk>

The Data-to-Everything Platform

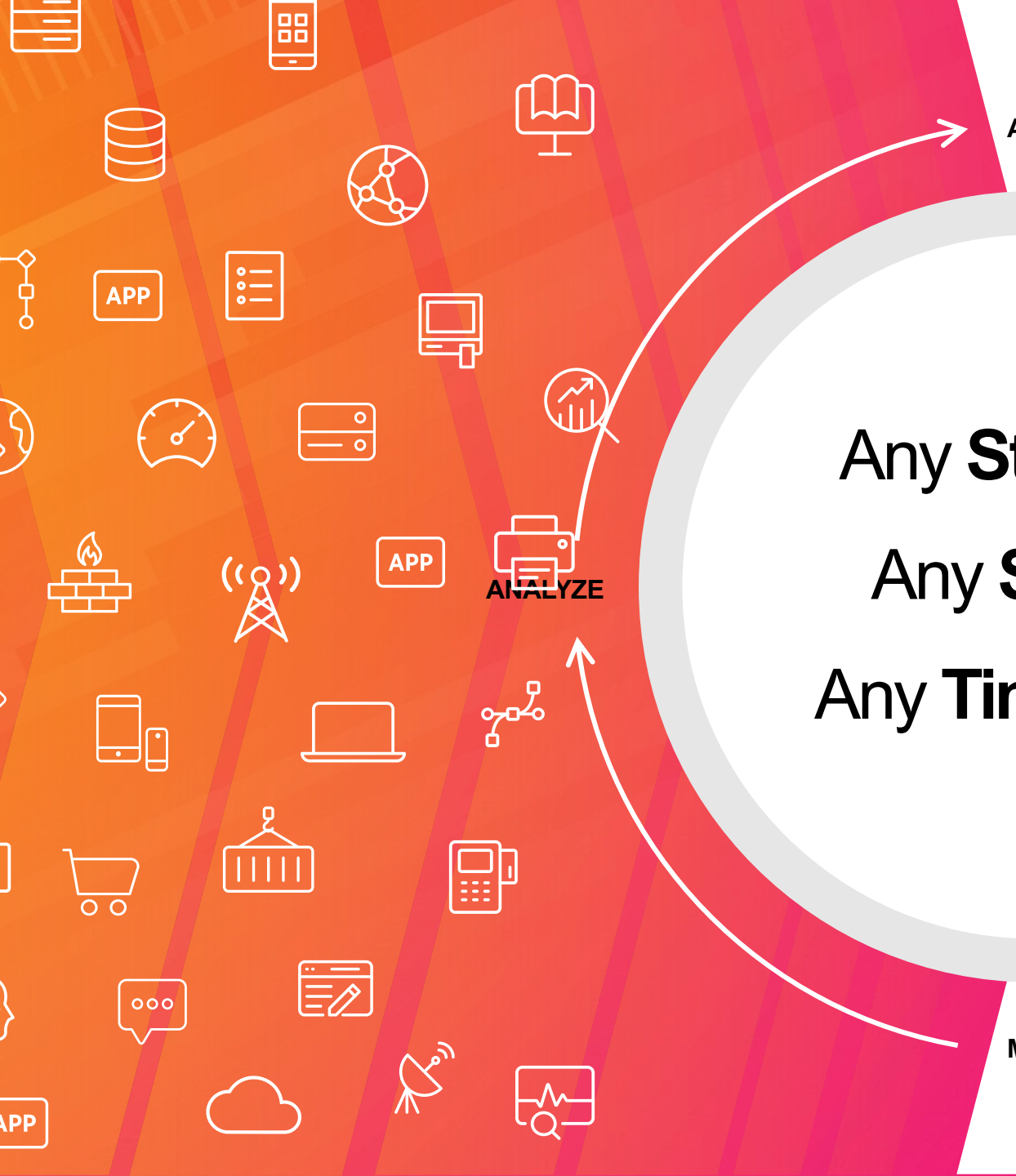
IT

Security

AppDev

Biz Analytics

splunk> turn data into doing



ACT

ANALYZE

INVESTIGATE

MONITOR

Any **Structure**

Any **Source**

Any **Time Scale**

IT

Security

AppDev

Biz Analytics

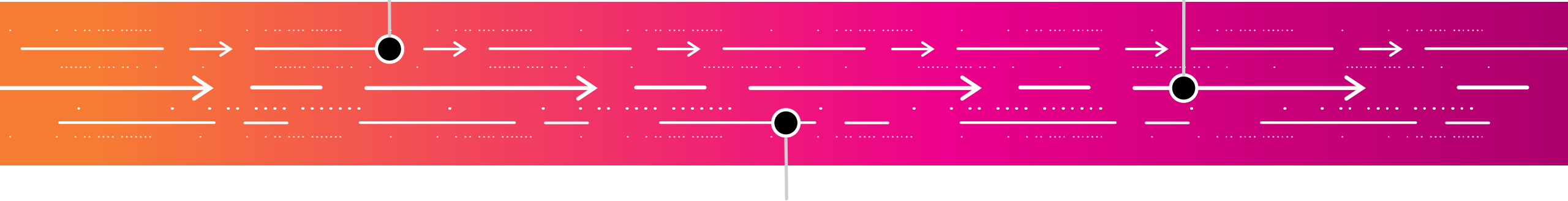
splunk> turn data into doing

Our Investigative Approach

Adaptable | Real-Time | Fast To Value | Massive Scale

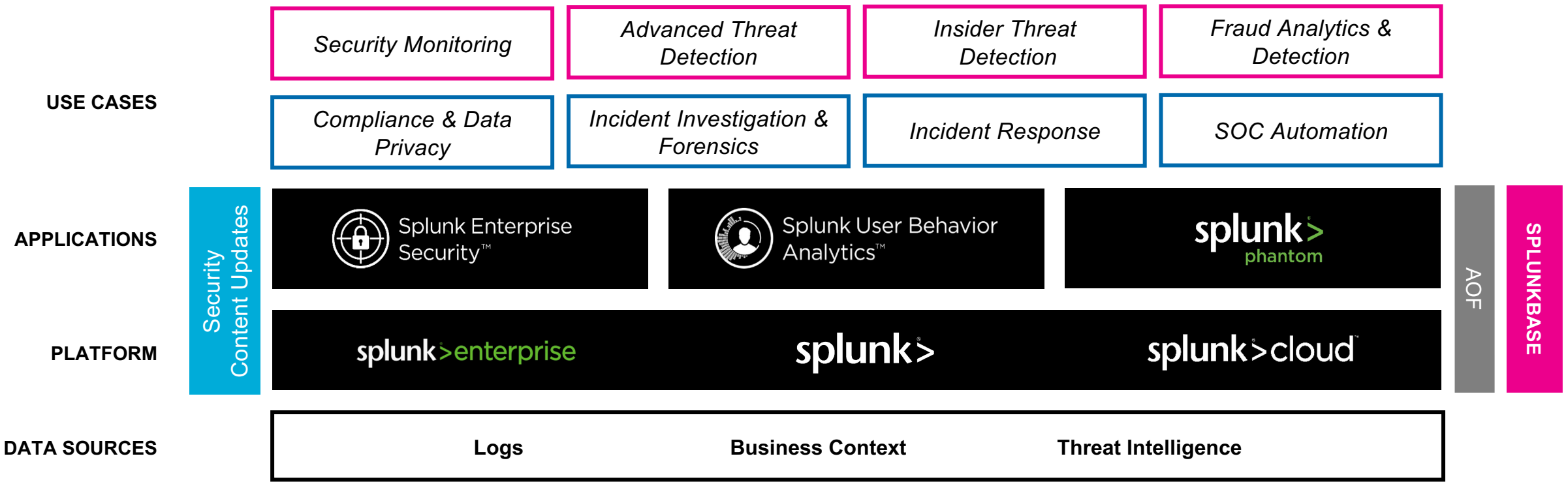
Send
unstructured data from all systems, devices, and people

React
quickly to changing circumstances by asking questions immediately

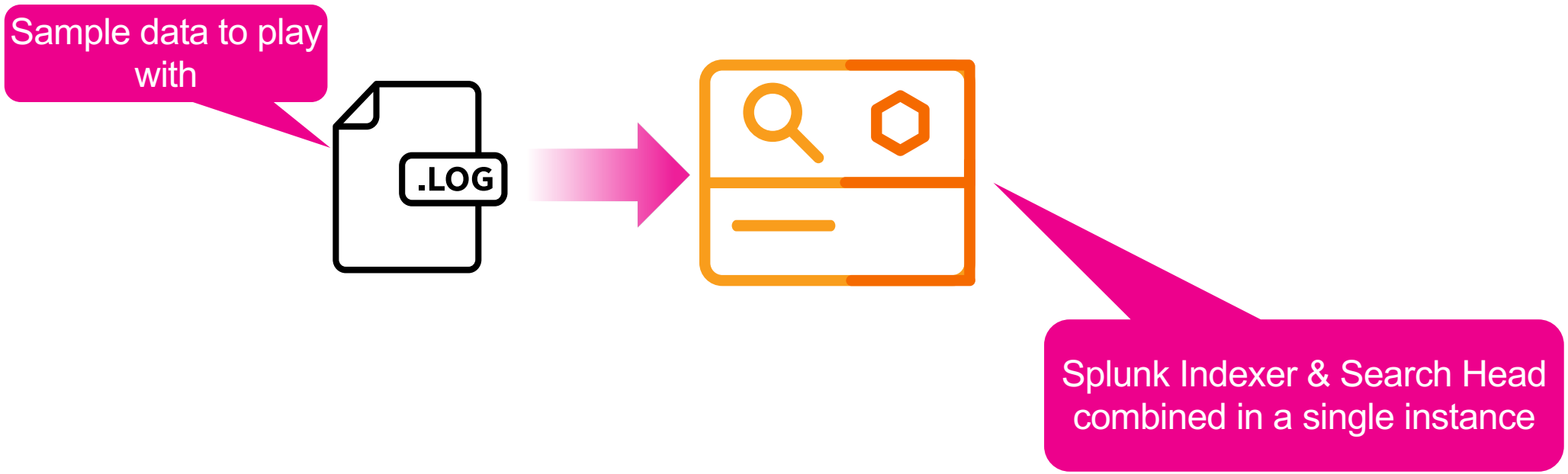


Don't Structure
your data until you are ready

Security Operations Suite

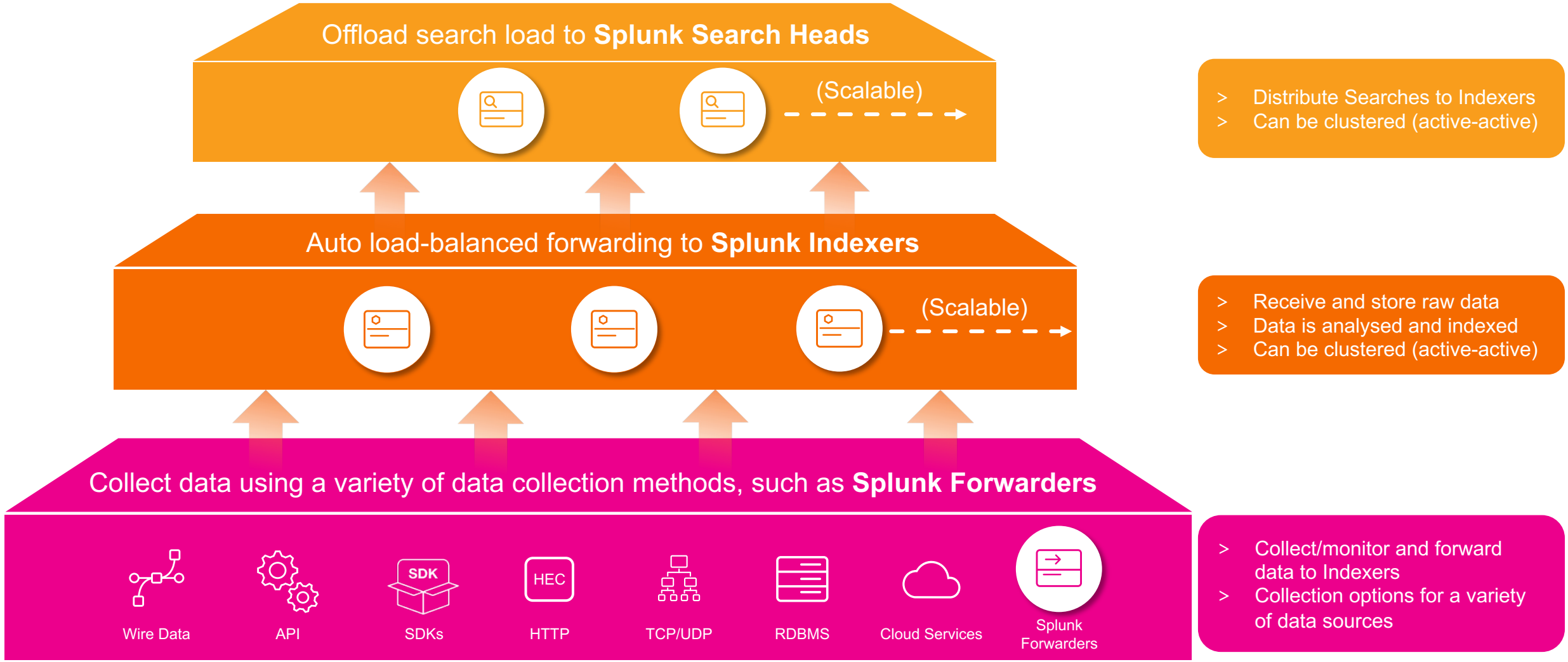


Today's Environment



Scales to Petabytes Per Day

Enterprise-Class Scale, Resilience and Interoperability



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

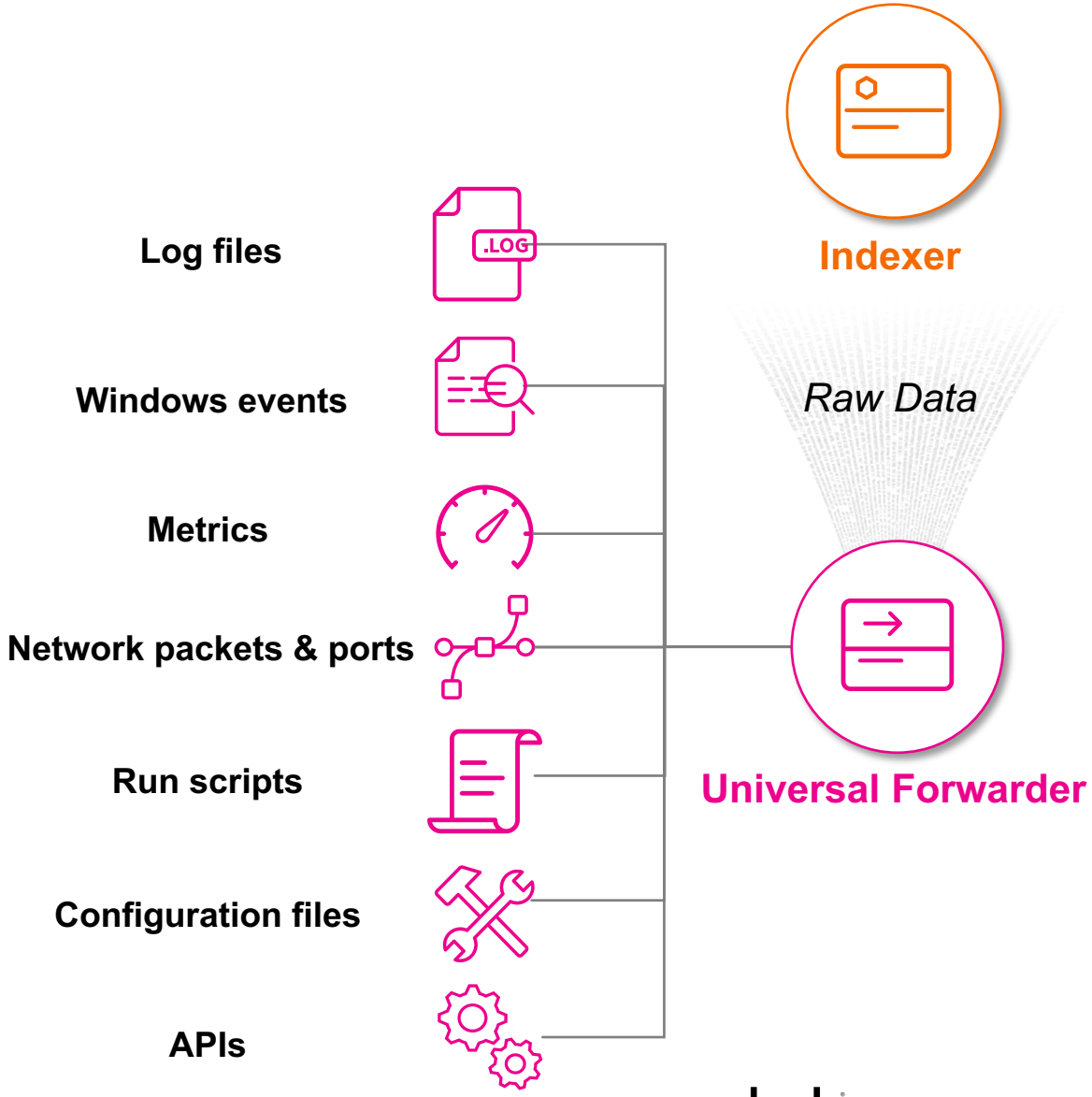
> Receive and store raw data
> Data is analysed and indexed
> Can be clustered (active-active)

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

splunk> turn data into doing

What is a Universal Forwarder?

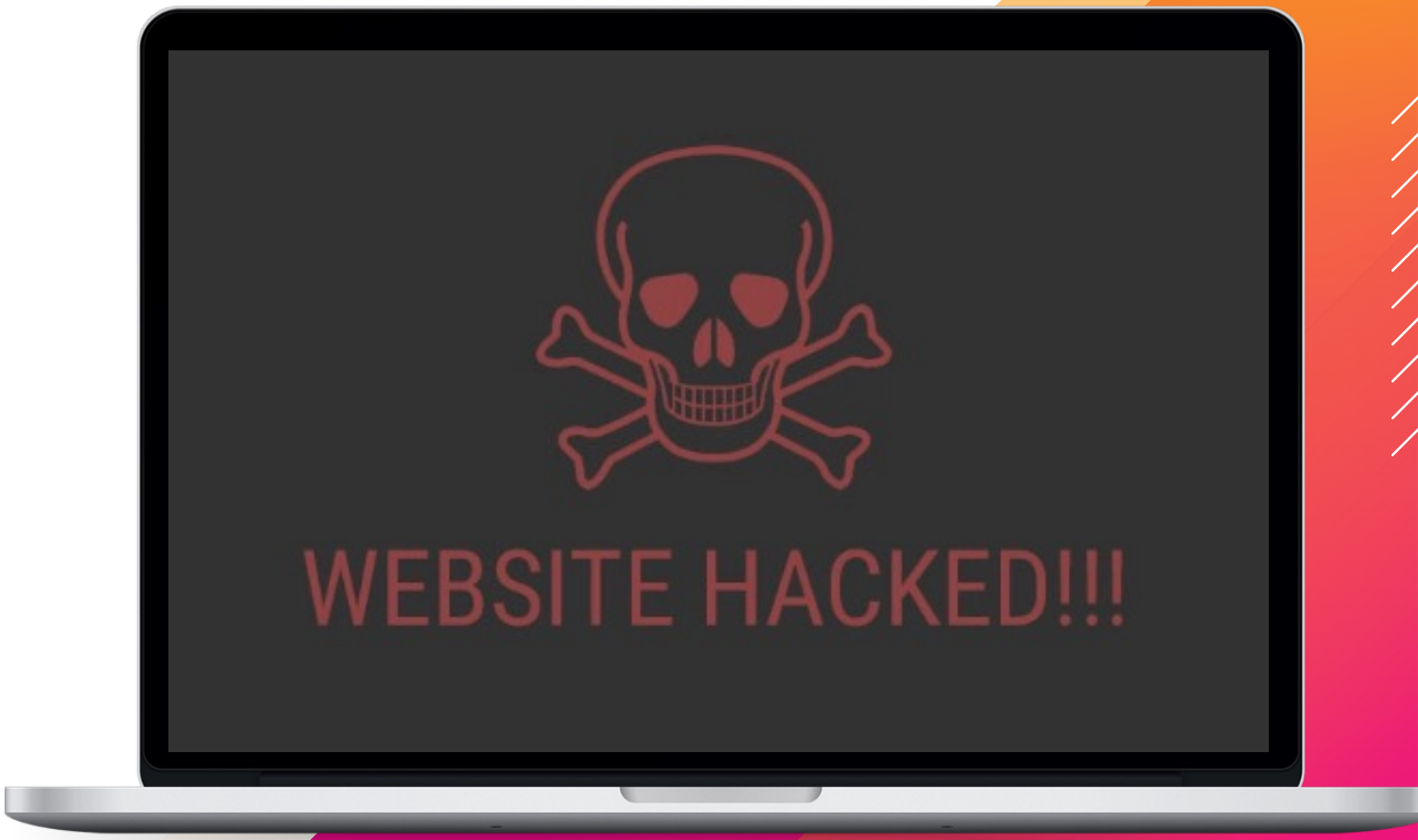
- Reliable collection of data from remote locations
- Includes methods for collecting from a variety of data sources
- Simple, but packed with lots of goodness:
  - ✓ Buffering / guaranteed delivery
  - ✓ Encryption
  - ✓ Compression
  - ✓ Load balancing
  - ✓ And more!
- Very small footprint
- Just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



imreallynotbatman.com

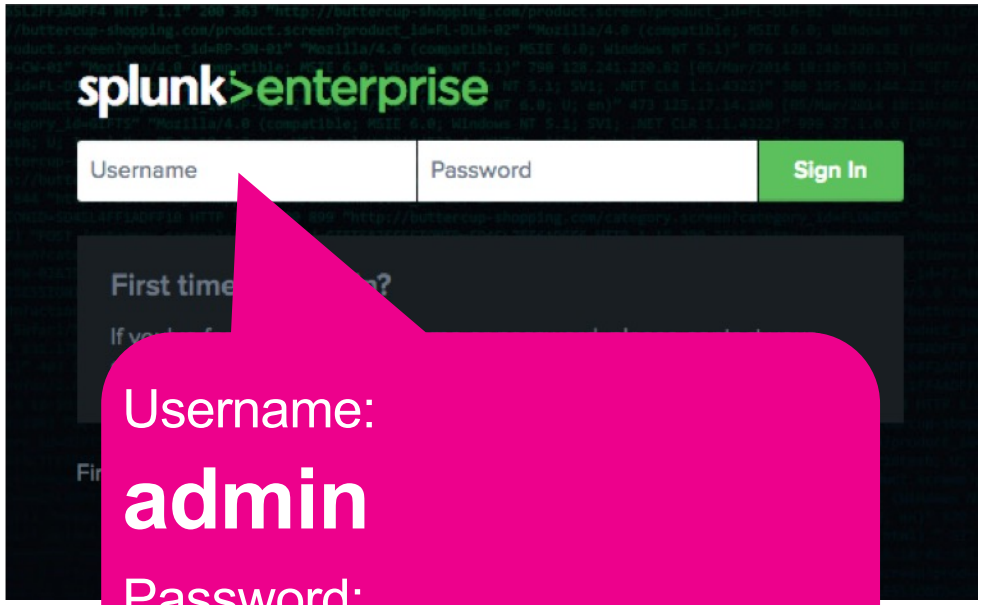
Security Data and Searches

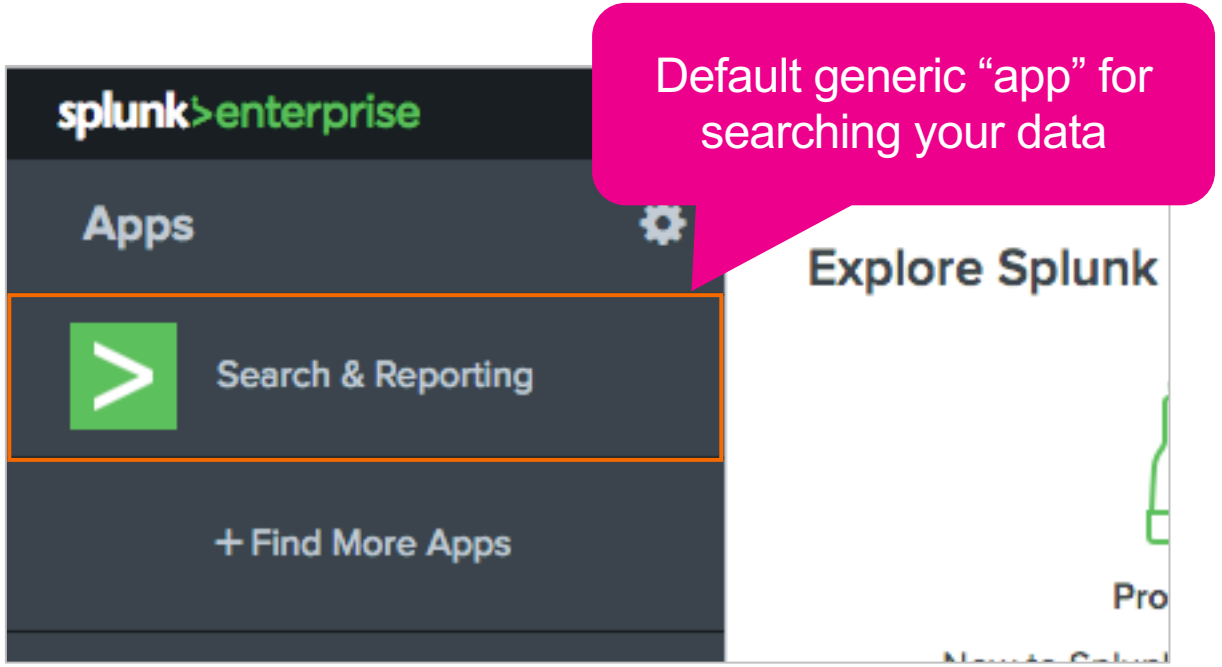
For Security People



Let’s Go!

Log in to Splunk





Search Basics

Using SPL & Navigating the Splunk Search Bar

Search Basics

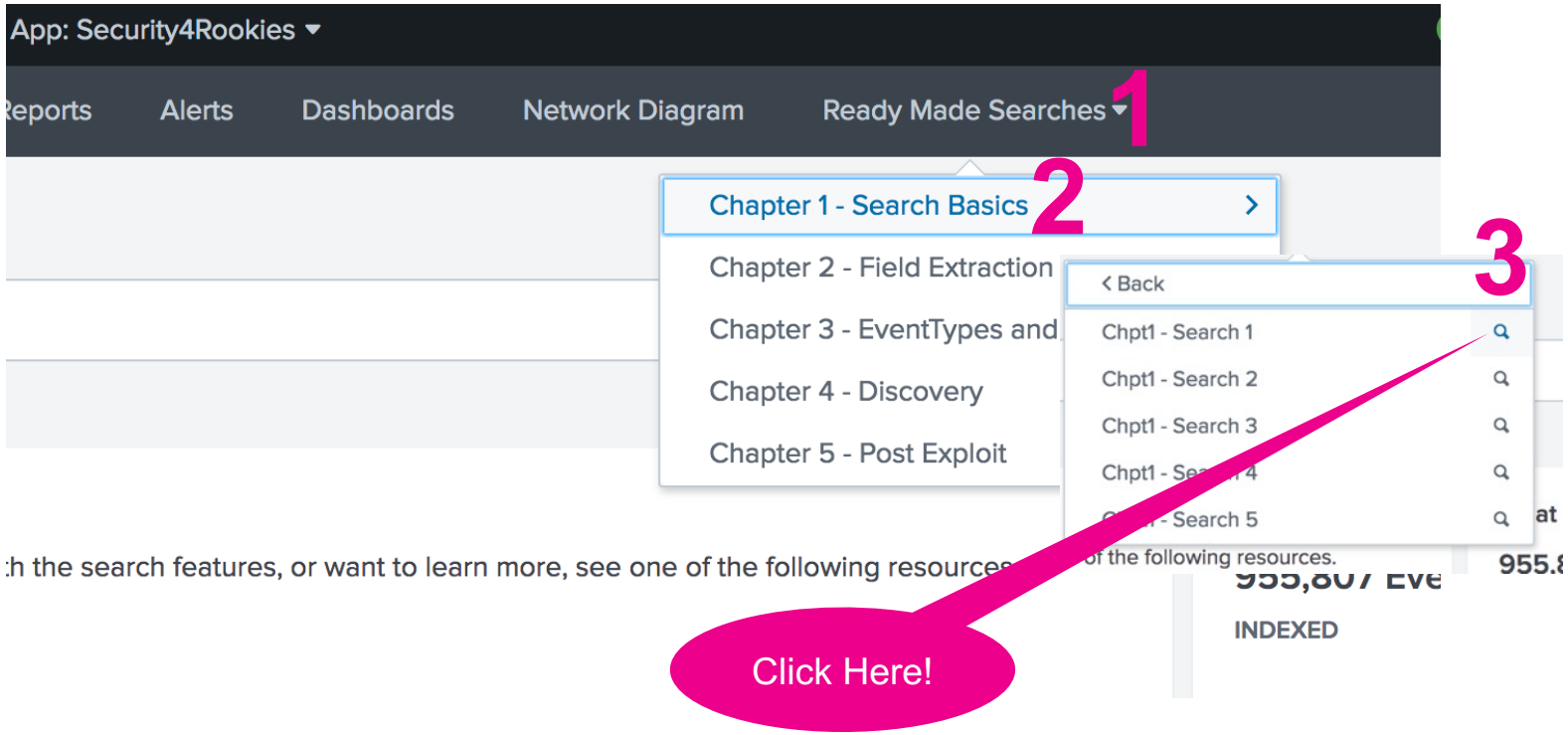
RULEZ for Searching

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

Easy Button!

All the searches we show today have been pre-typed for you.

Don’t want to type? No problem!



splunk> turn data into doing

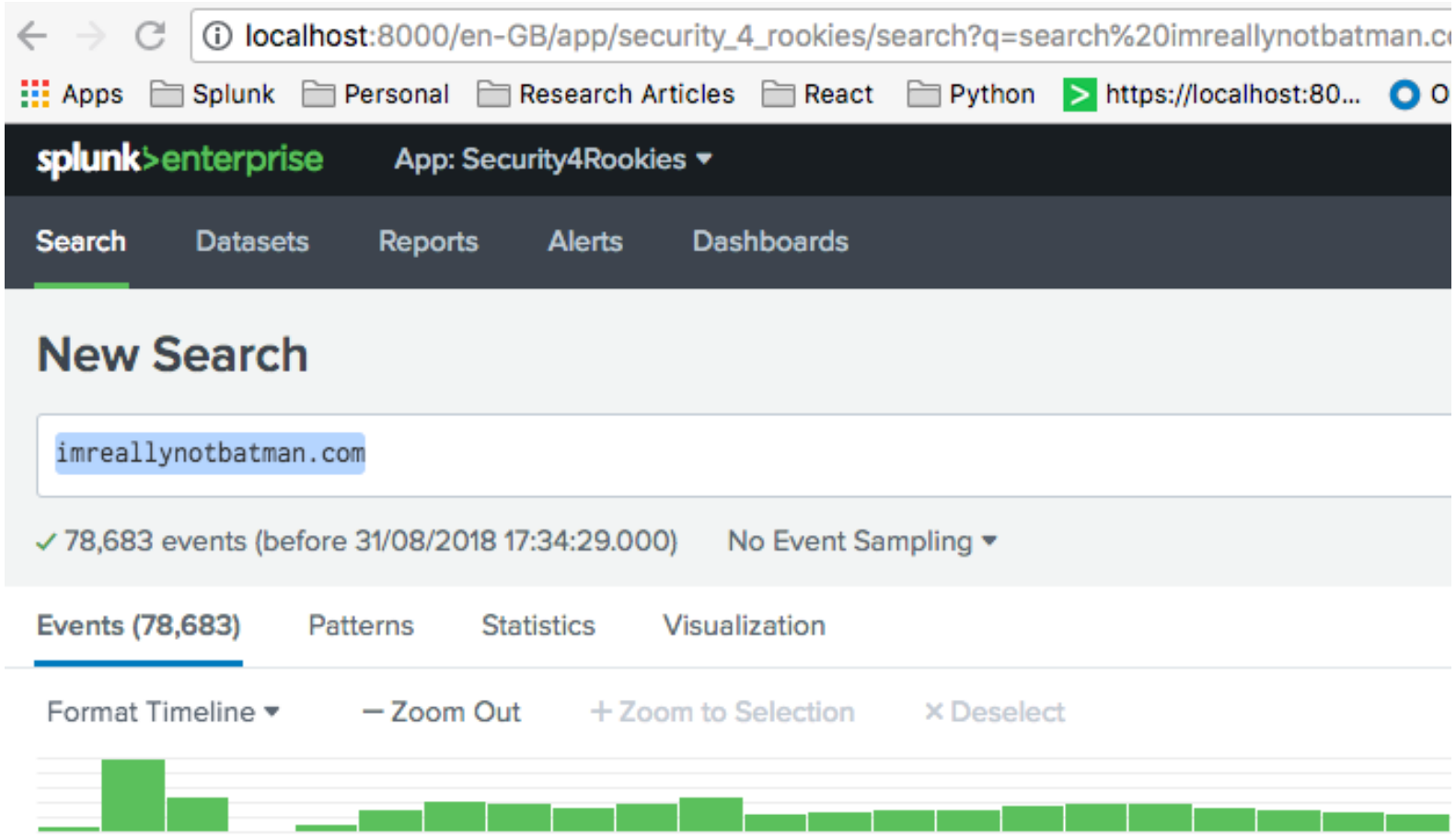
Search Basics

Chpt1 – Search 1

Literal Strings

Manual

imreallynotbatman.com



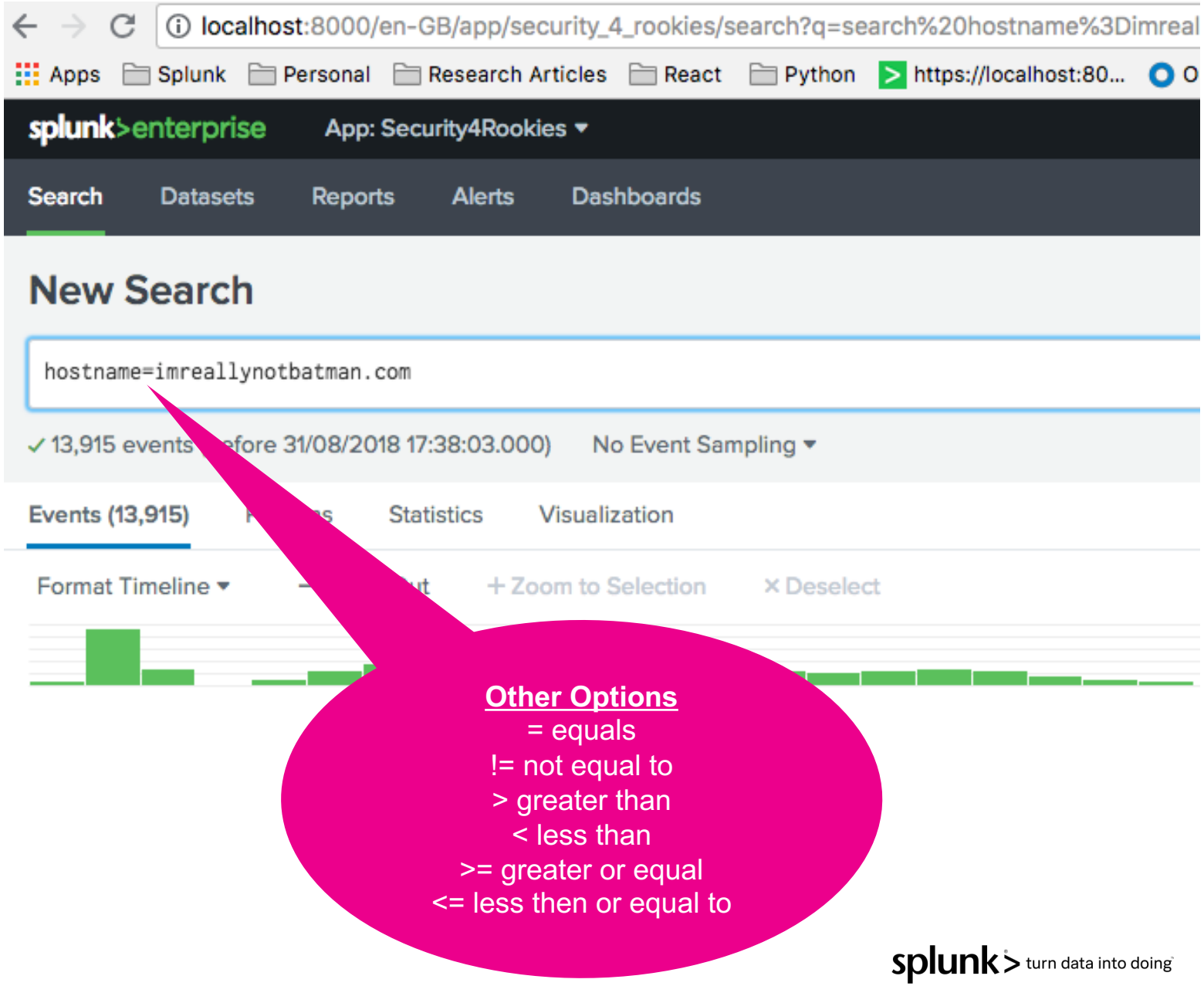
Search Basics

Chpt1 – Search 2

Key=Value pair searching

Manual

hostname="imreallynotbatman.com"



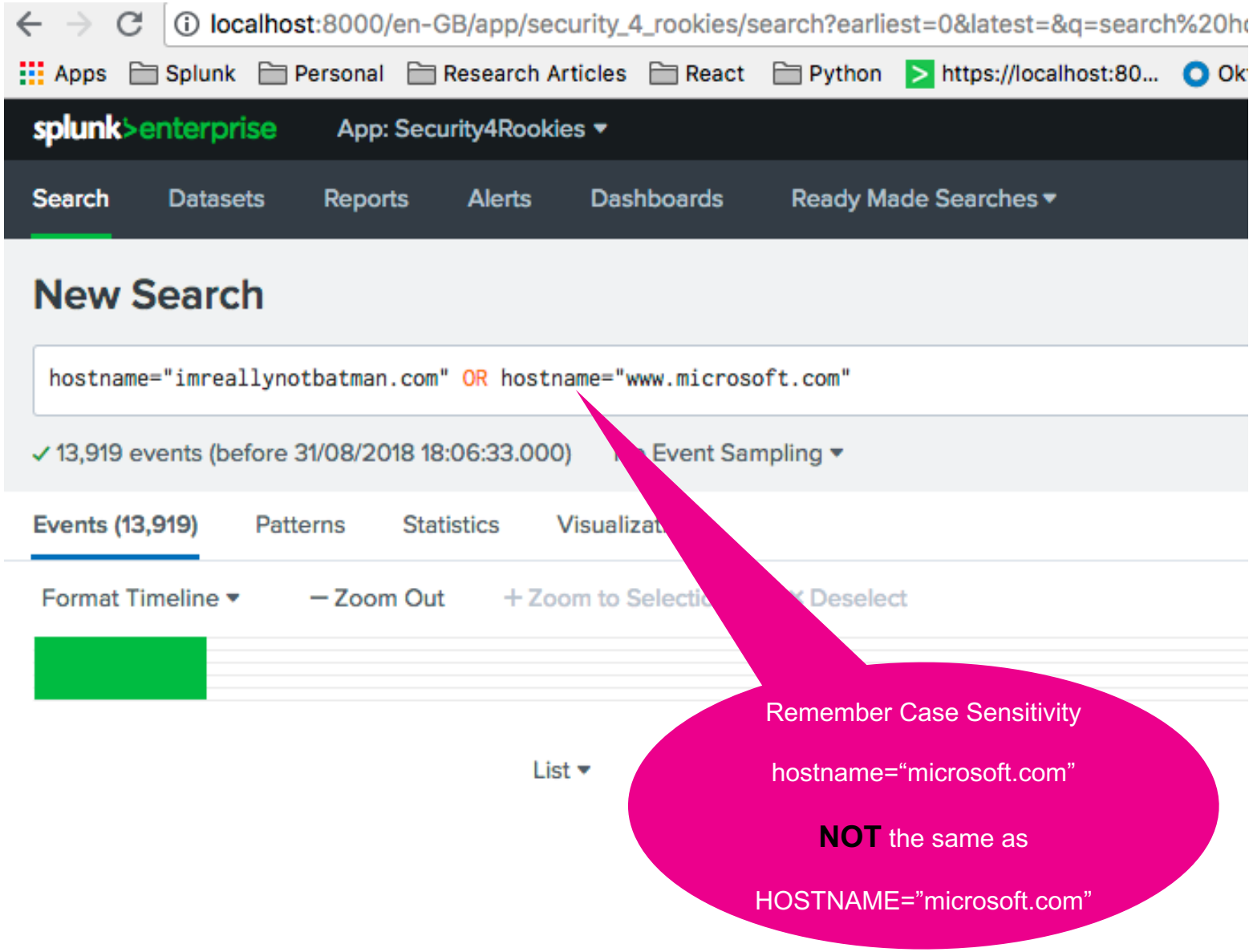
Search Basics

Chpt1 – Search 3

Using OR

Manual

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



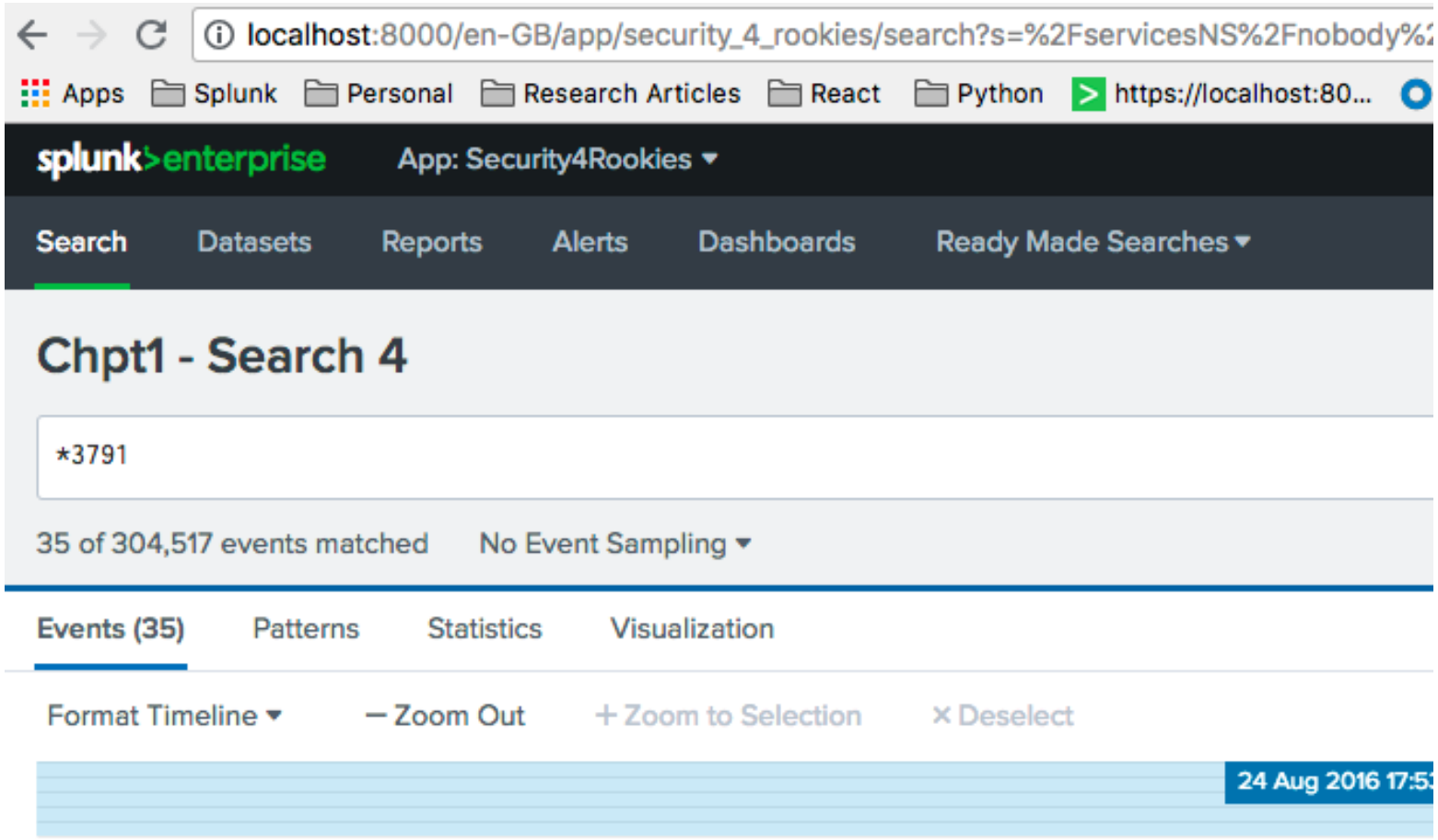
Search Basics

Chpt1 – Search 4

Using Wildcards

Manual

*3791



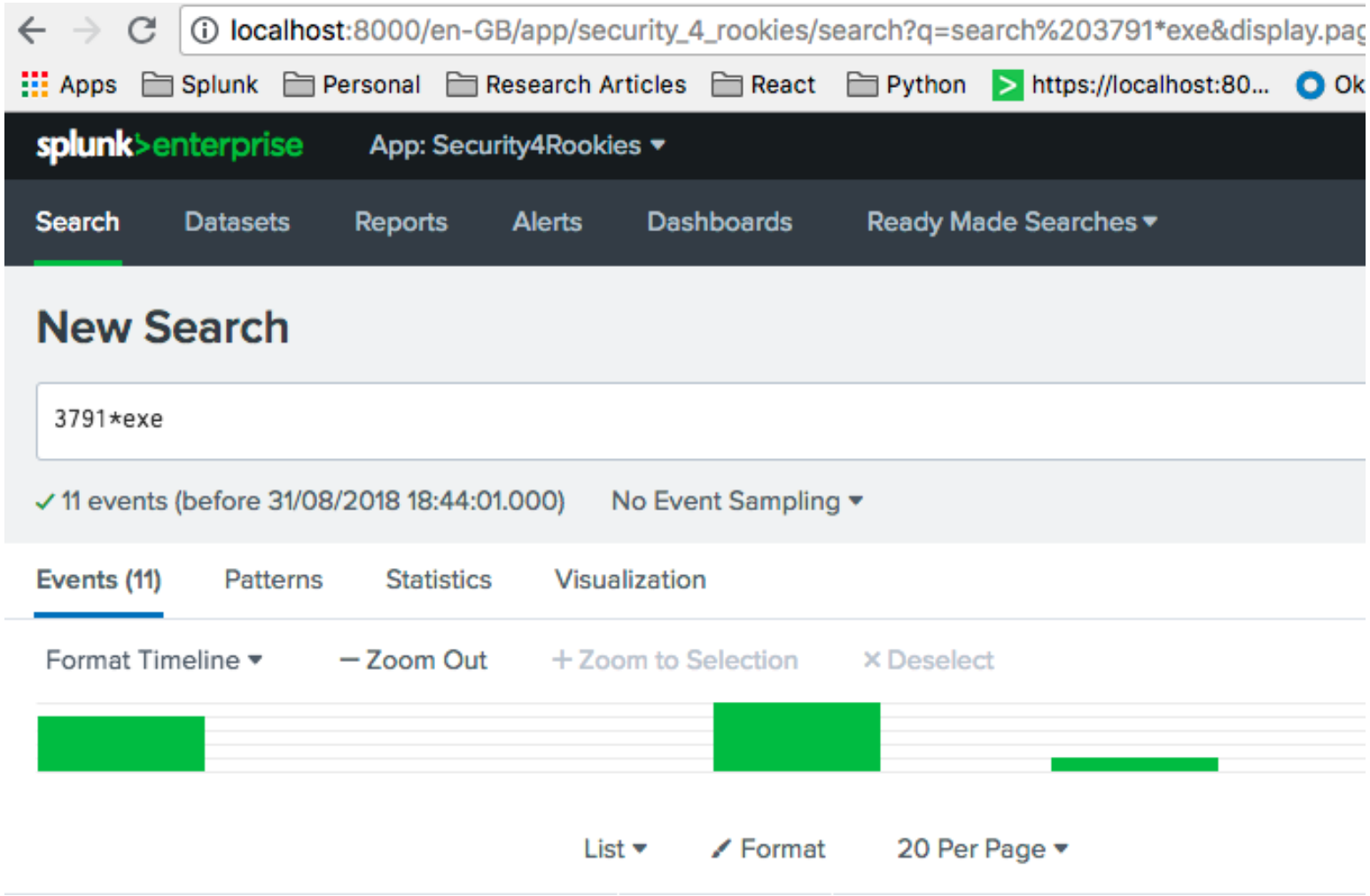
Search Basics

Chpt1 – Search 5

Using Wildcards

Manual

3791*exe



Search Basics

Chpt1 – Search 6

CIDR Matching

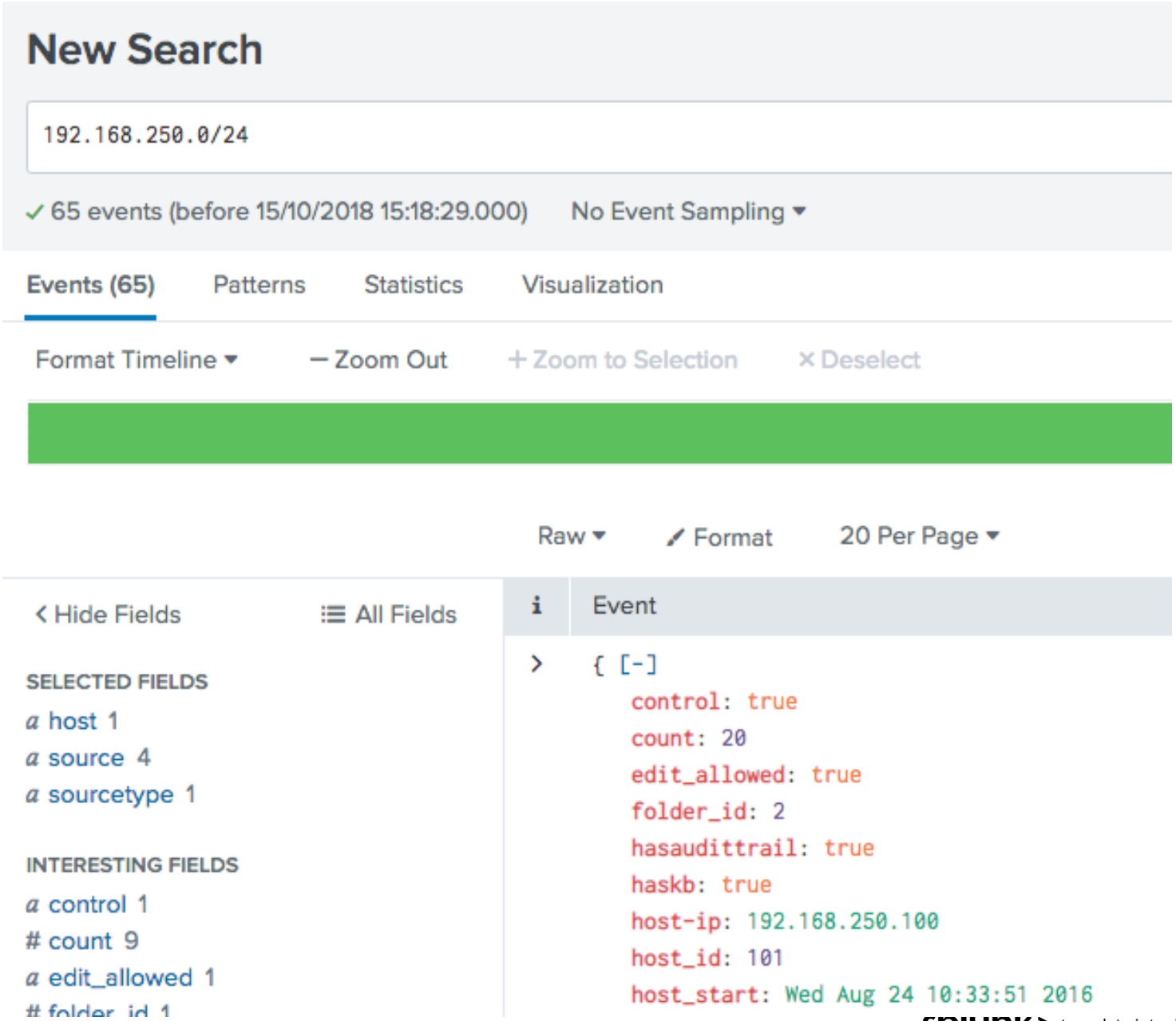
Manual

192.168.250.0/24

Also try

dest_ip=192.168.250.0/24

Could also key=value search
dest_ip=192.168.250.0/24



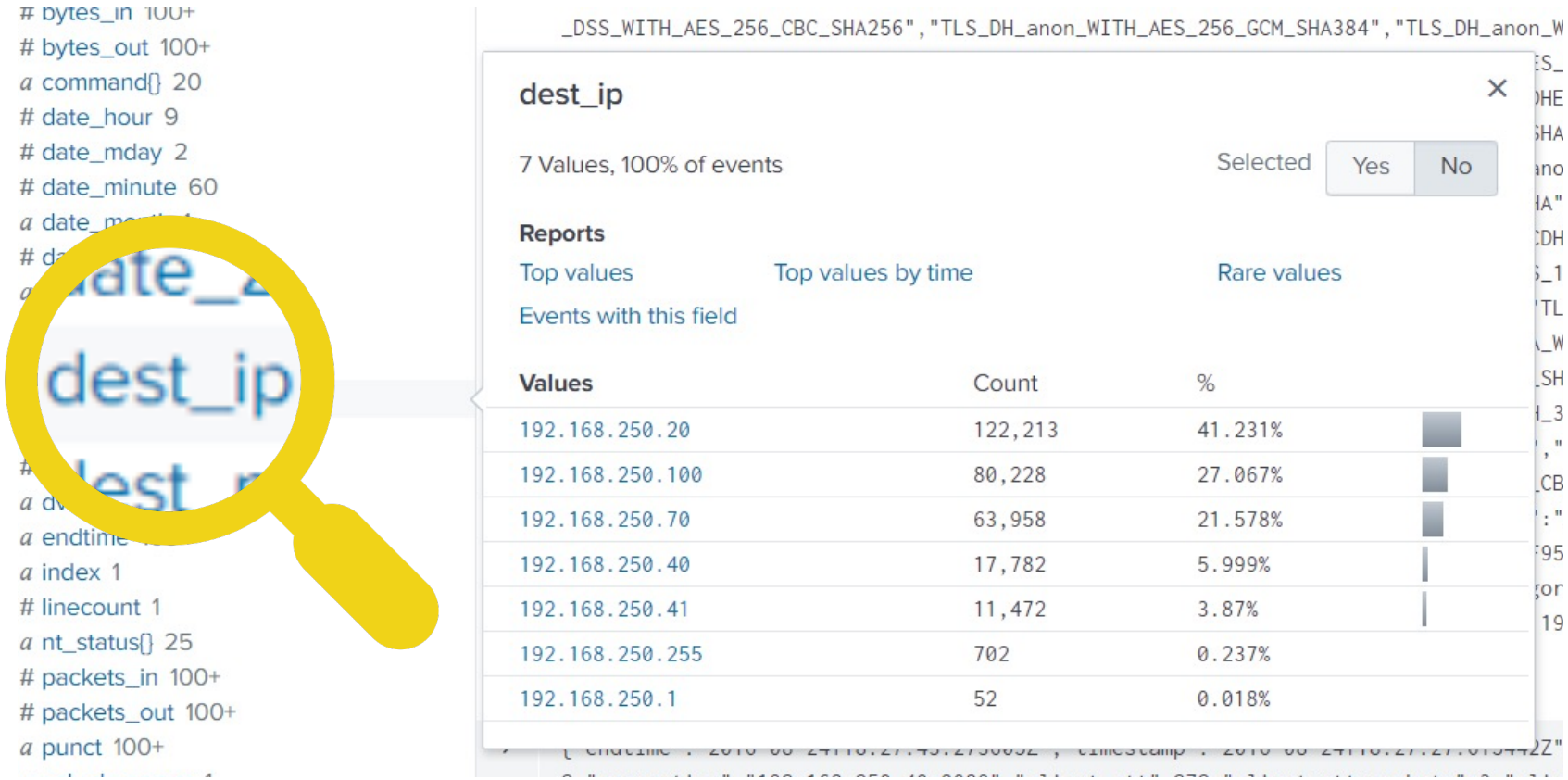
Search Basics

Chpt1 – Search 6

CIDR Matching

Manual

dest_ip=192.168.250.0/24



Splunk's 'Search Processing Language' (SPL)

Search terms

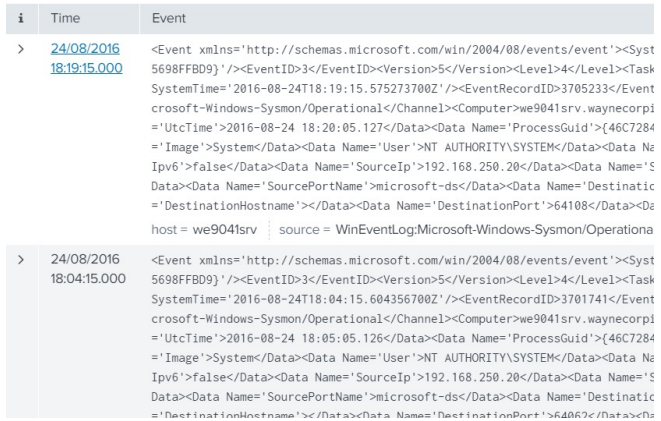
Commands

```
dest_ip=192.168.250.70 | 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`



Time	Event
24/08/2016 18:19:15.000	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><Syst 5698FFBD9}'/><EventID>3</EventID><Version>5</Version><Level>4</Level><Task SystemTime='2016-08-24T18:19:15.575273700Z'/><EventRecordID>3705233</Event crosoft-Windows-Sysmon/Operational</Channel><Computer>we9041srv.waynecorpi ='UtcTime'>2016-08-24 18:20:05.127</Data><Data Name='ProcessGuid'>{46C7284 ='Image'>System</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Na Ipv6'>false</Data><Data Name='SourceIp'>192.168.250.20</Data><Data Name='S Data><Data Name='SourcePortName'>microsoft-ds</Data><Data Name='Destinatic ='DestinationHostname'></Data><Data Name='DestinationPort'>64108</Data><Da host = we9041srv source = WinEventLog:Microsoft-Windows-Sysmon/Operationa
24/08/2016 18:04:15.000	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><Syst 5698FFBD9}'/><EventID>3</EventID><Version>5</Version><Level>4</Level><Task SystemTime='2016-08-24T18:04:15.604356700Z'/><EventRecordID>3701741</Event crosoft-Windows-Sysmon/Operational</Channel><Computer>we9041srv.waynecorpi ='UtcTime'>2016-08-24 18:05:05.126</Data><Data Name='ProcessGuid'>{46C7284 ='Image'>System</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Na Ipv6'>false</Data><Data Name='SourceIp'>192.168.250.20</Data><Data Name='S Data><Data Name='SourcePortName'>microsoft-ds</Data><Data Name='Destinatic

`| 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:** http://bit.ly/S4R-QuickRef

> **Splunk Docs:** https://docs.splunk.com

splunk> turn data into doing

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

Indexing Basics

Where the Data Meets Controls

Indexing Basics

RULEZ for Indexes

1. Indexes are repositories on your indexer
2. A logical way to segregate data
3. Access Control is done on Indexes
4. Data Retention controlled per Index
5. Use them to speed up your searches!

Sourcetype Basics

Where you define the format of your data!

Sourcetype Basics

RULEZ for Sourcetypes

1) Categorically the single most important part of getting your data into Splunk

2) Categorically the single most important part of getting your data into Splunk

3) Categorically the single most important part of getting your data into Splunk

Sourcetype Basics

RULEZ for Sourcetypes

Revisited

1) How Splunk knows where to break events

2) How to extract fields from each event

3) What data manipulation occurs for each event

4) ALL config is stored under the sourcetype name

Sourcetype Basics

RULEZ for Sourcetypes

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=elevat
```

fortigate:utm

Single Line Breaking
Key=Value pair Extractions

Extracting Fields Basics

Where you make your data useable

Field Extraction Basics

RULEZ for Field Extraction

1) Technology Addons are your fastest route (splunkbase.splunk.com) – search Technology AddOns

2) Check automatically recognized sourcetypes (http://docs.splunk.com/Documentation/Splunk/latest/Data/Listofpretrainedsourcetypes)

3) Key=Value works out the box – use field aliasing if you want to rename

4) UI based extraction when 1 – 3 didn't come through for you

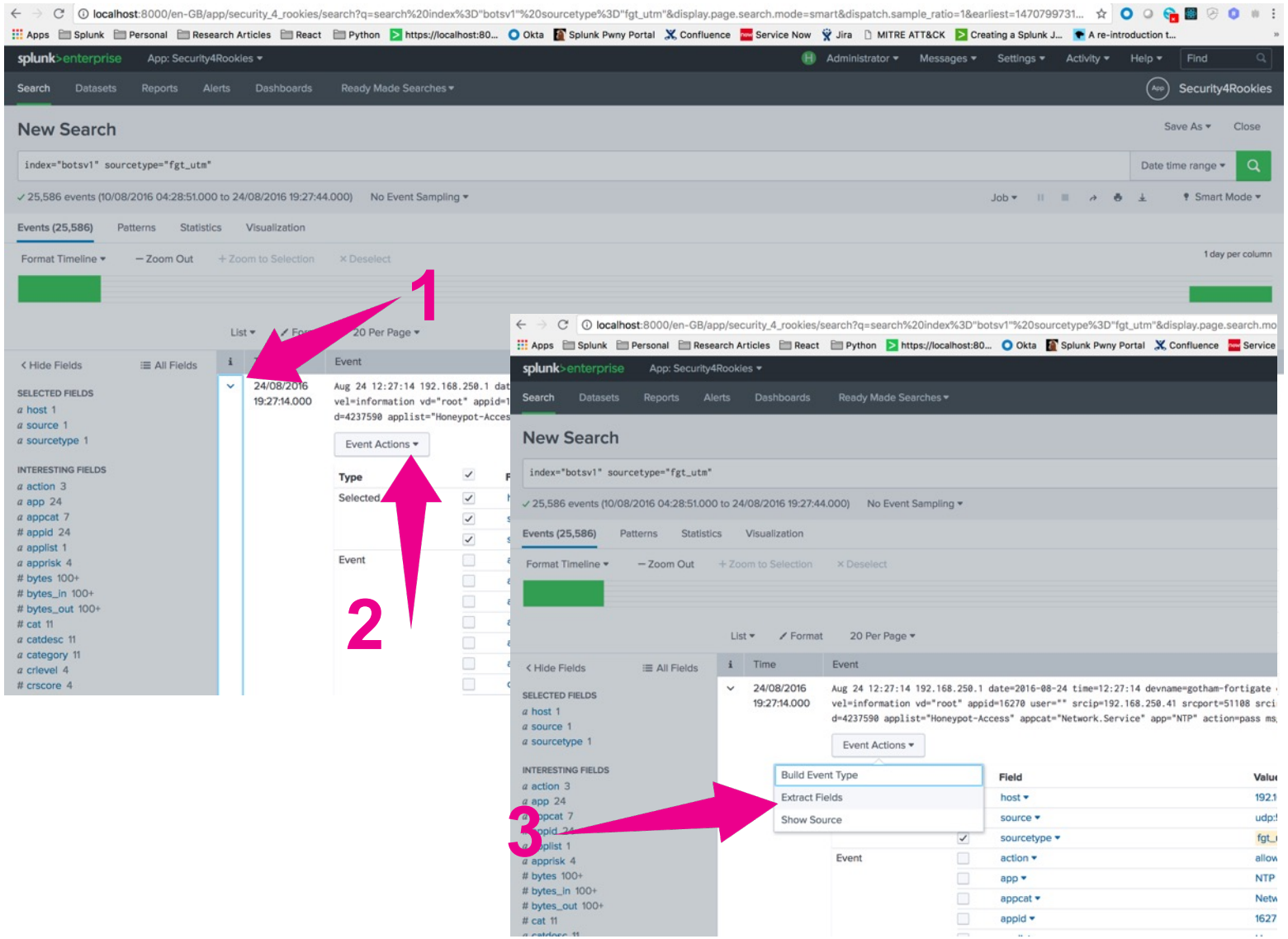
Field Extraction Basics

Chpt2 – Search 1

Search your data source

Manual

index=botsv1 sourcetype=fgt_utm

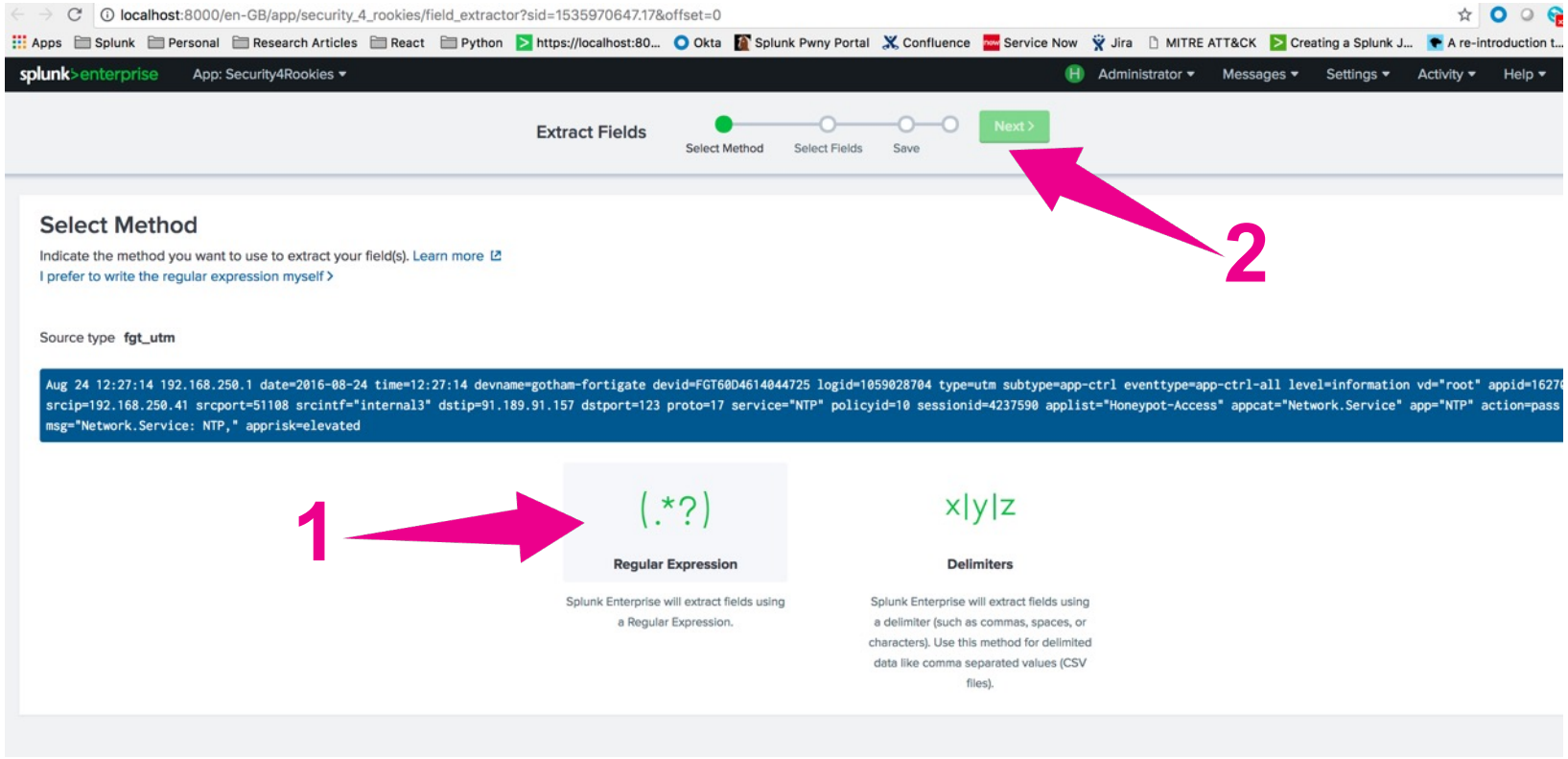


splunk> turn data into doing

Field Extraction Basics

Chpt2 – Search 1

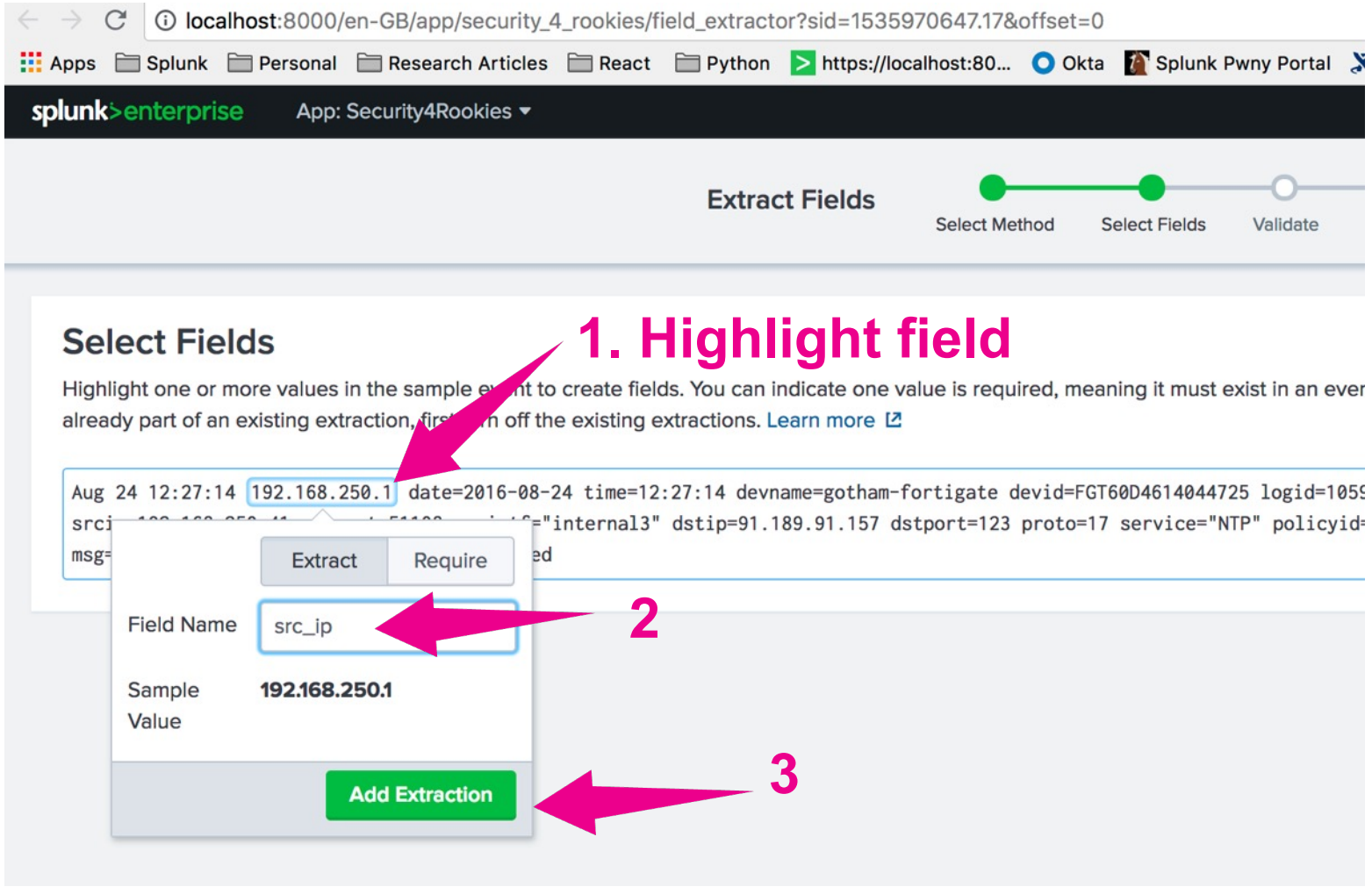
Extract the field



Field Extraction Basics

Chpt2 – Search 1

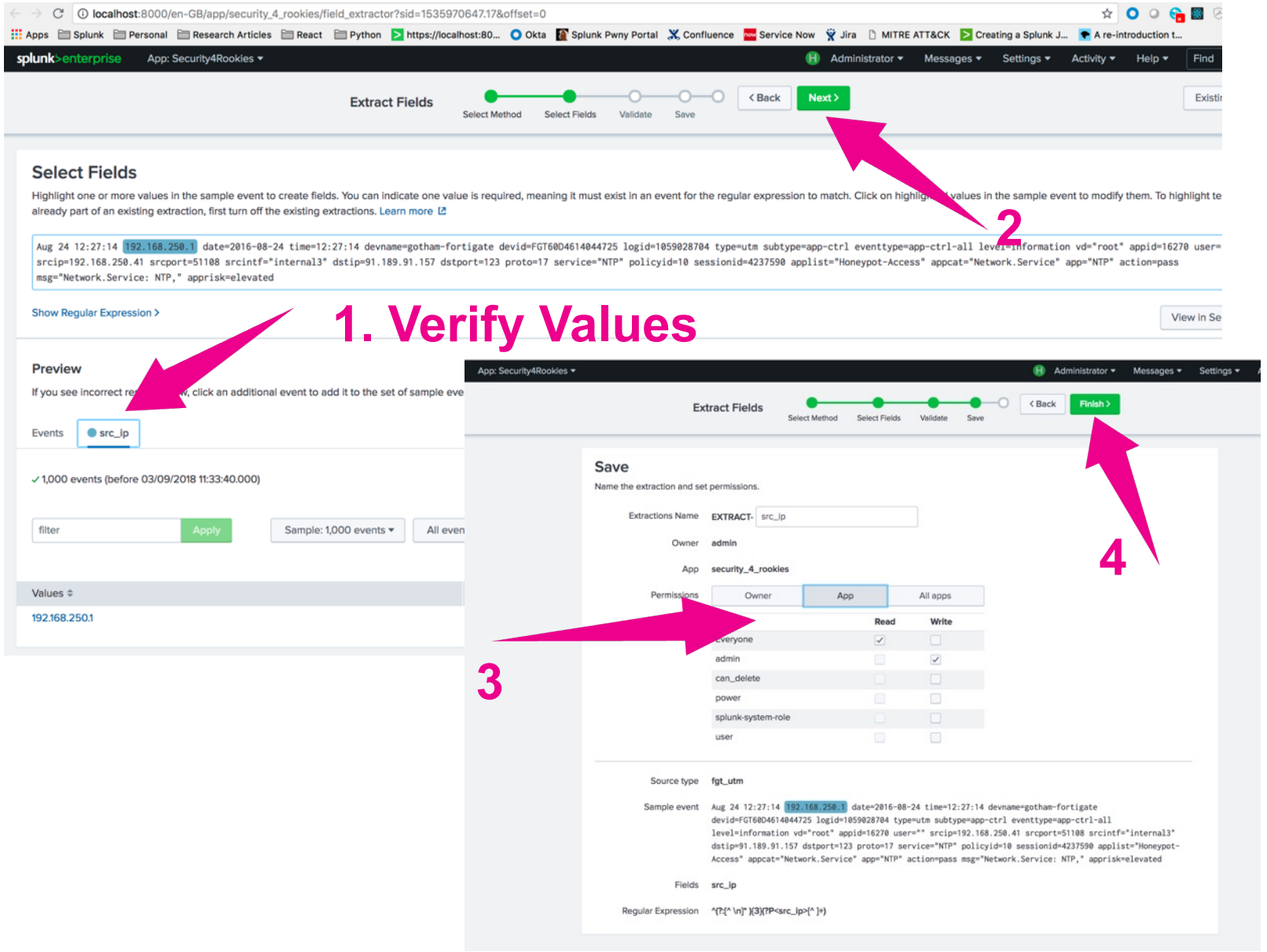
Highlight and Name



Field Extraction Basics

Chpt2 – Search 1

Verify Fields and Set Access Rights



splunk> turn data into doing

Event Types & Tags Basics

Where you make correlated data at scale

Event Types & Tags Basics

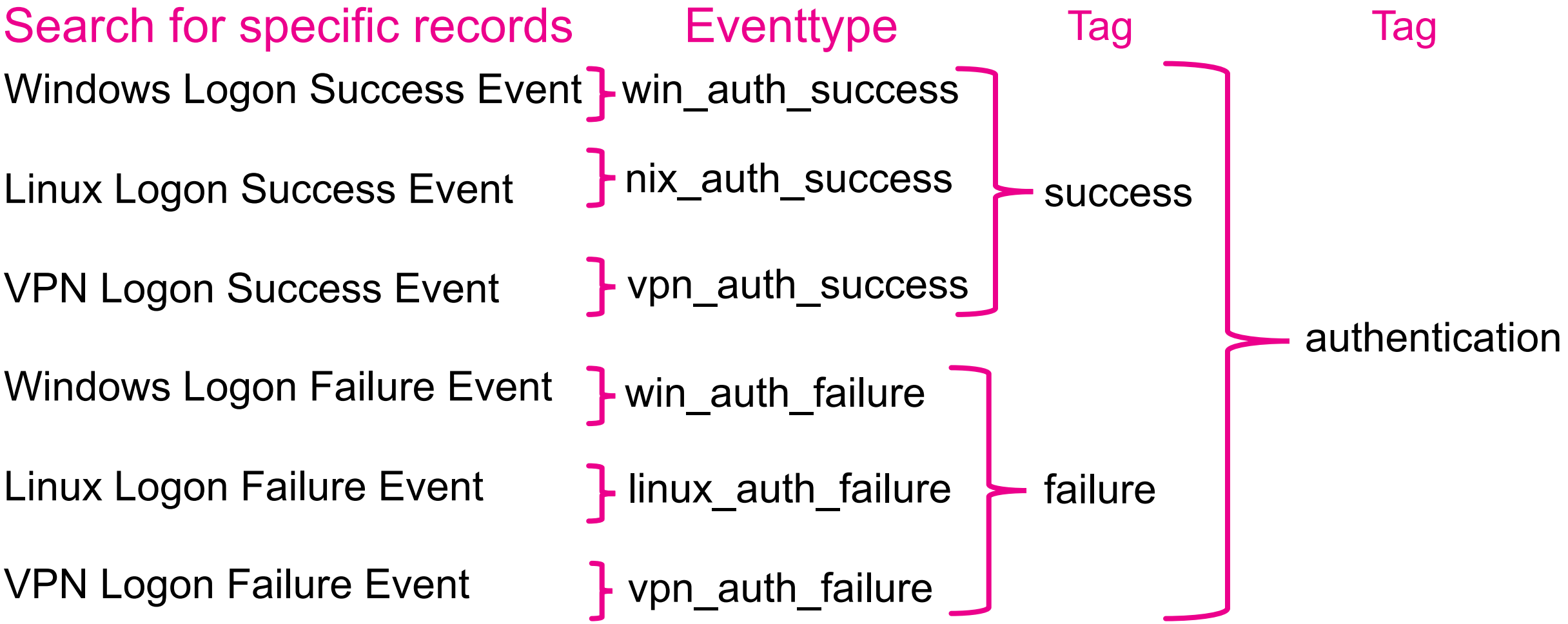
RULEZ for Event Types & Tags

1) Event types are created to categorize specific events within a sourcetype

2) Tags are abstractions over the top of event types

Correlating Events

Using EventTypes and Tags



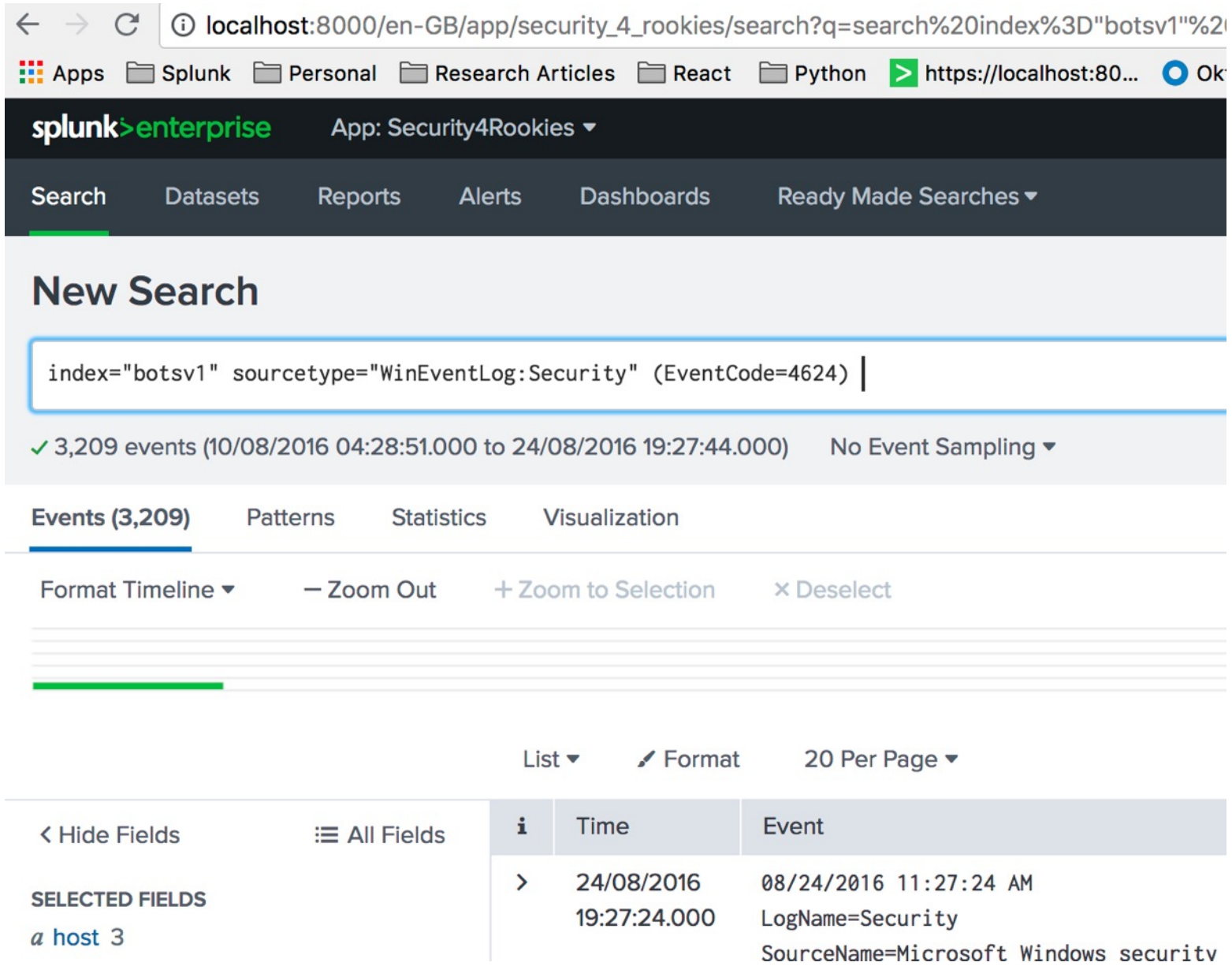
Event Types & Tags Basics

Chpt3 – Search 1

Creating an Eventtype

Manual

index=botsv1
sourcetype=WinEventLog:Security
(EventCode=4624)



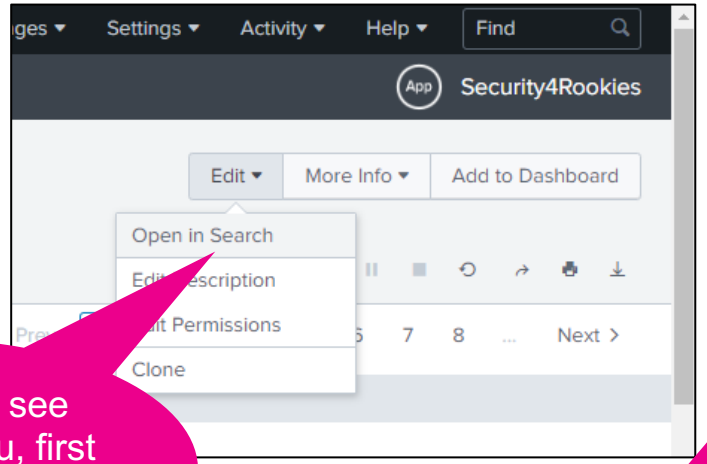
Event Types & Tags Basics

Chpt3 – Search 1

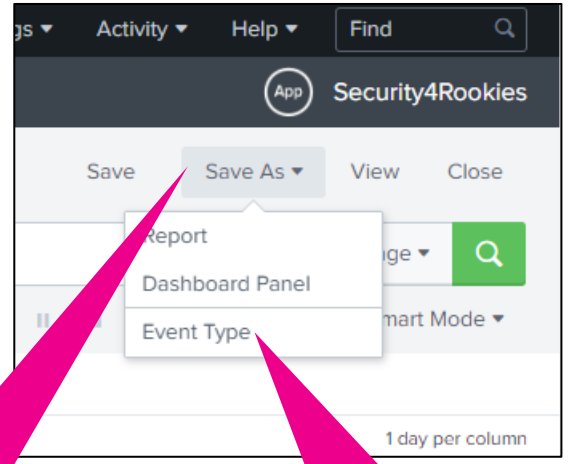
Creating an Eventtype

Manual

index=botsv1
sourcetype=WinEventLog:Security
(EventCode=4624)

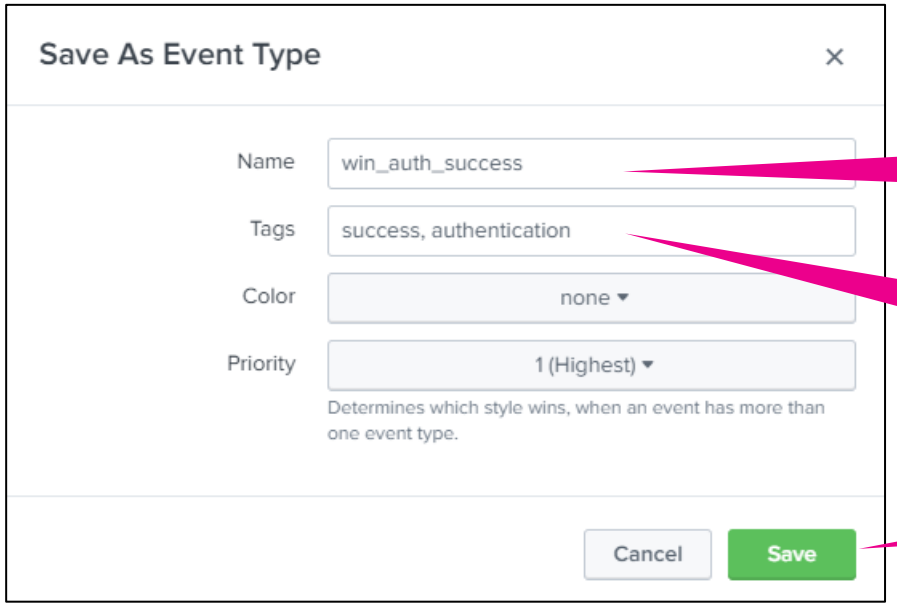


1. If you can't see "Save As" menu, first click "Edit" then "Open in Search"



2. "Save As"

3. "Event Type"



4. Enter Event Type name "win_auth_success"

5. Enter Tags (comma separated) "success, authentication"

6. "Save"

splunk> turn data into doing

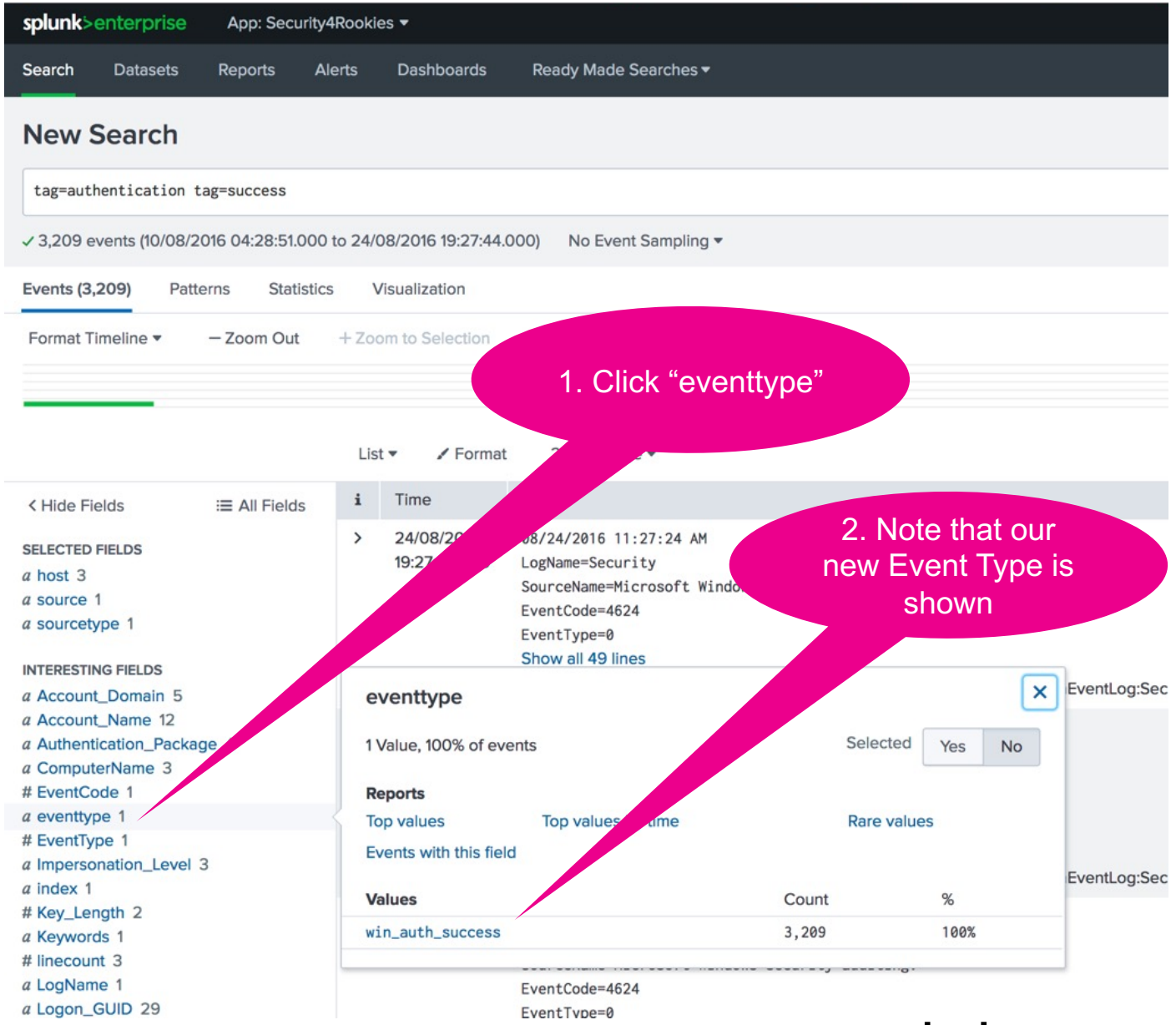
Event Types & Tags Basics

Chpt3 – Search 2

Searching by tags

Manual

tag=authentication tag=success



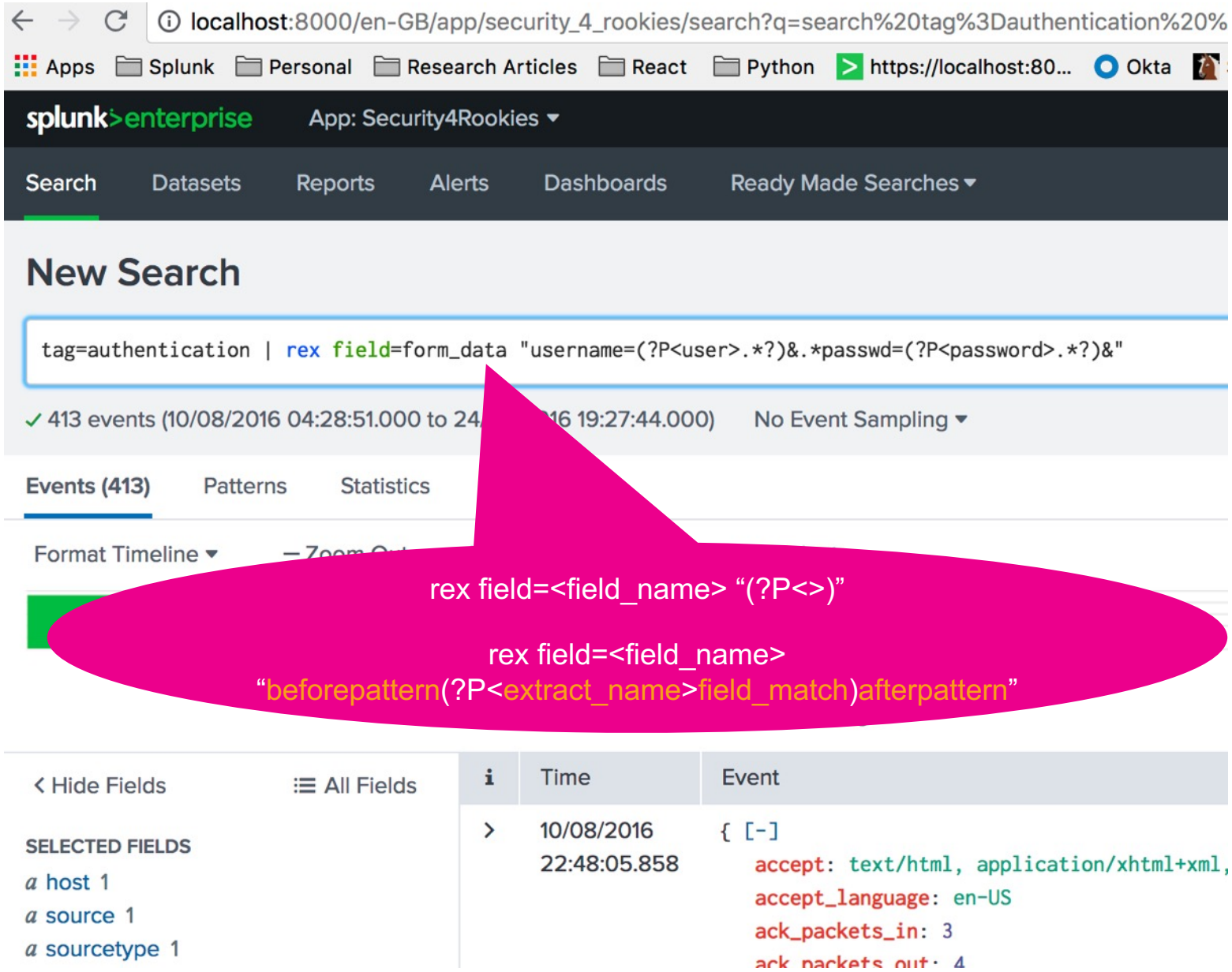
Bonus Material

Chpt3 – Search 3

REGEX for the brave

Manual

tag=authentication | rex field=form_data "username=(?P<user>.*?)&.*passwd=(?P<password>.*?)&"



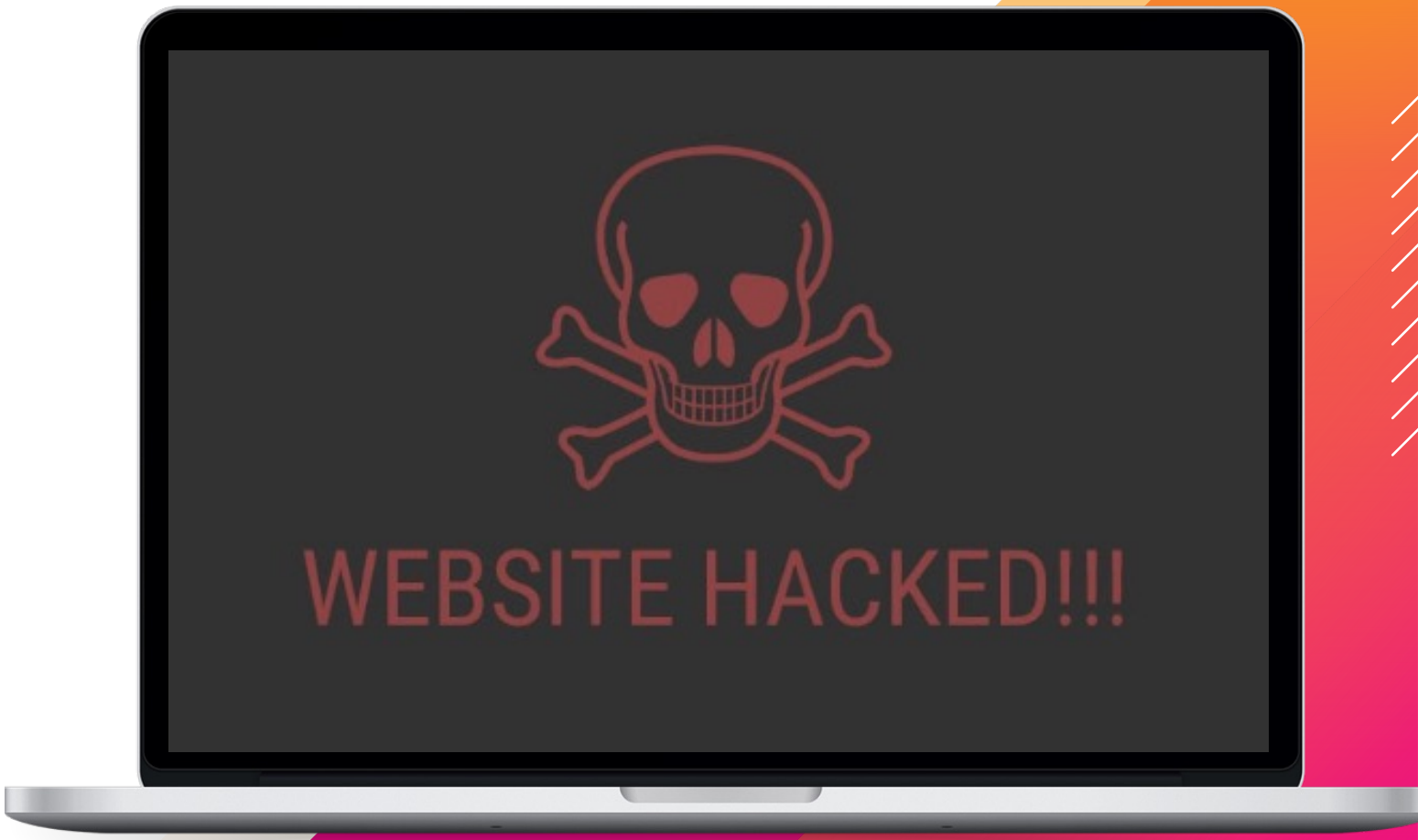
Plugging it all together

Where the rubber meets the road

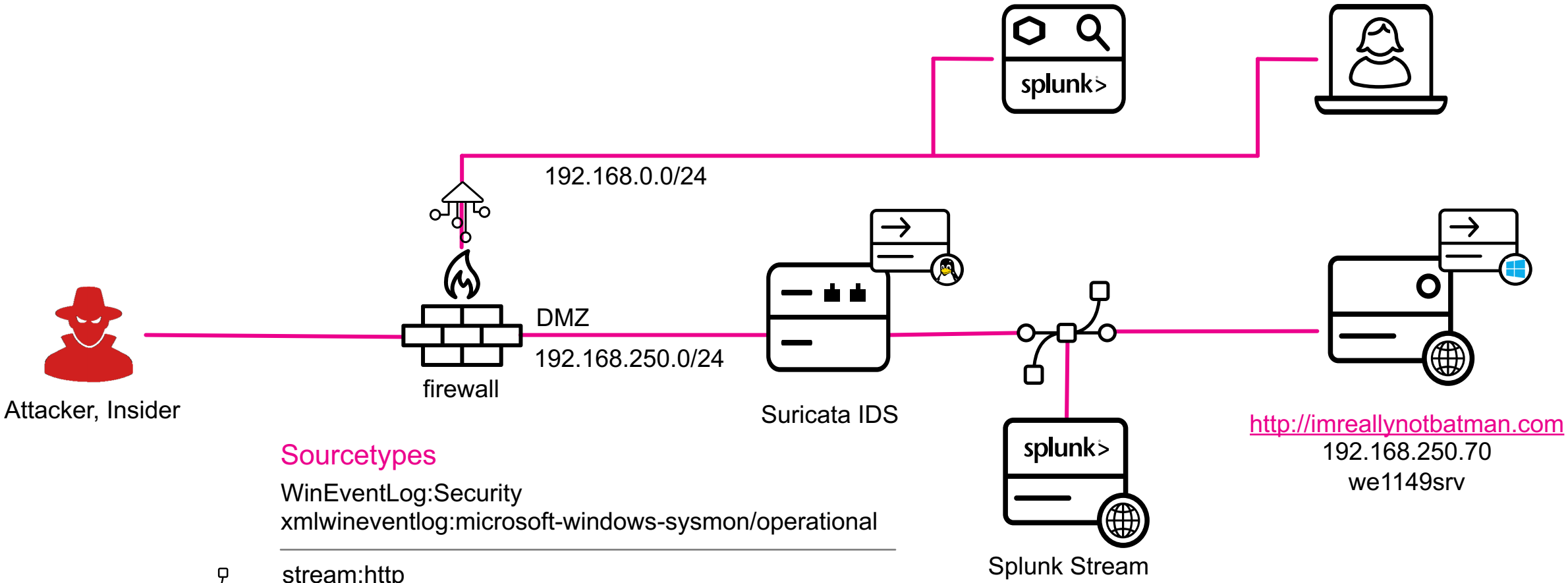
imreallynotbatman.com

Security Data and Searches

For Security People



WayneCorp Network



Sourcetypes

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

---

wire data

stream:http
stream:dns
stream:*

---

firewall

fgt_utm

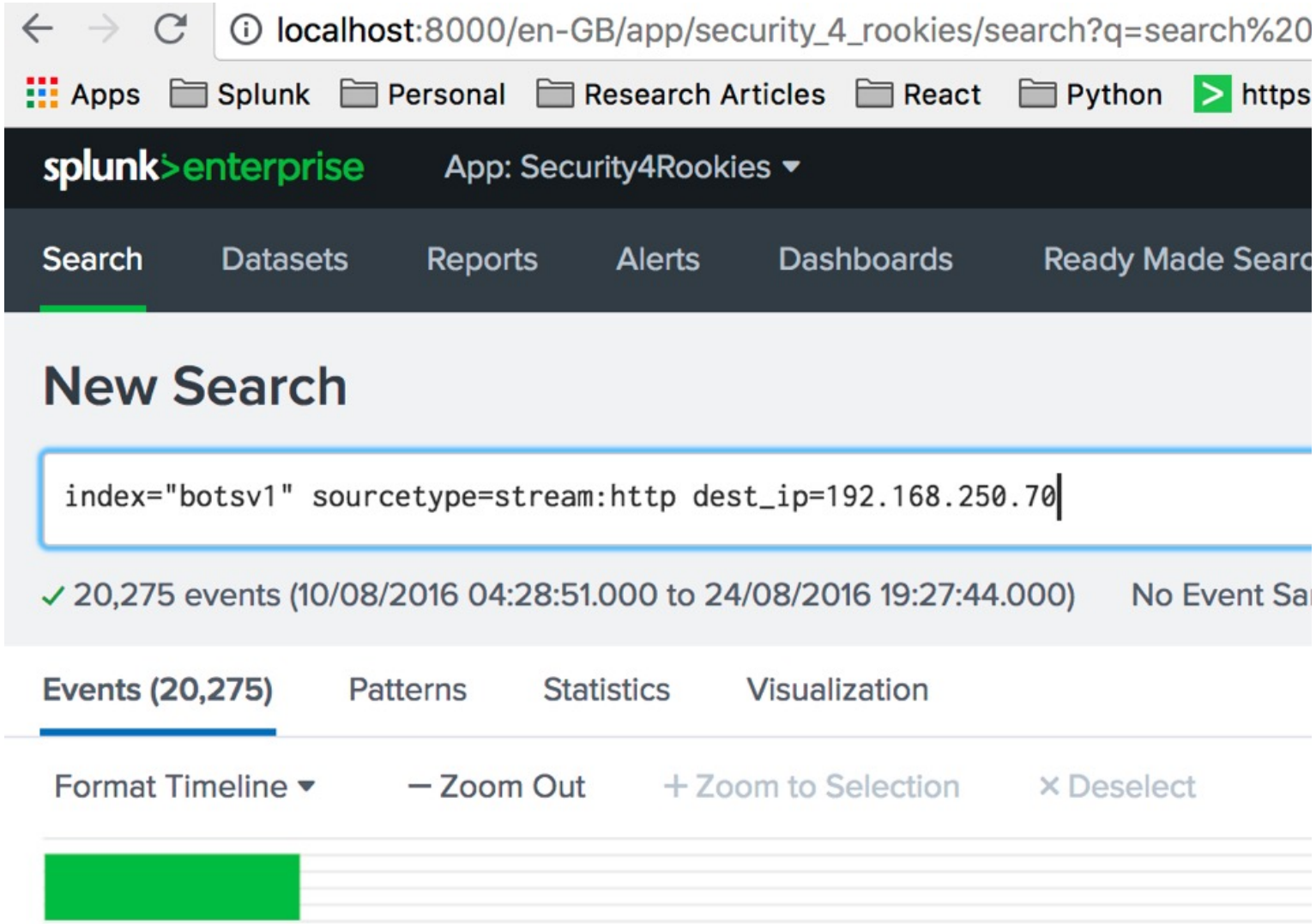
Discovering the attack

Chpt4 – Search 1

Filter traffic to the web server

Manual

index="botsv1" sourcetype=stream:http dest_ip=192.168.250.70



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

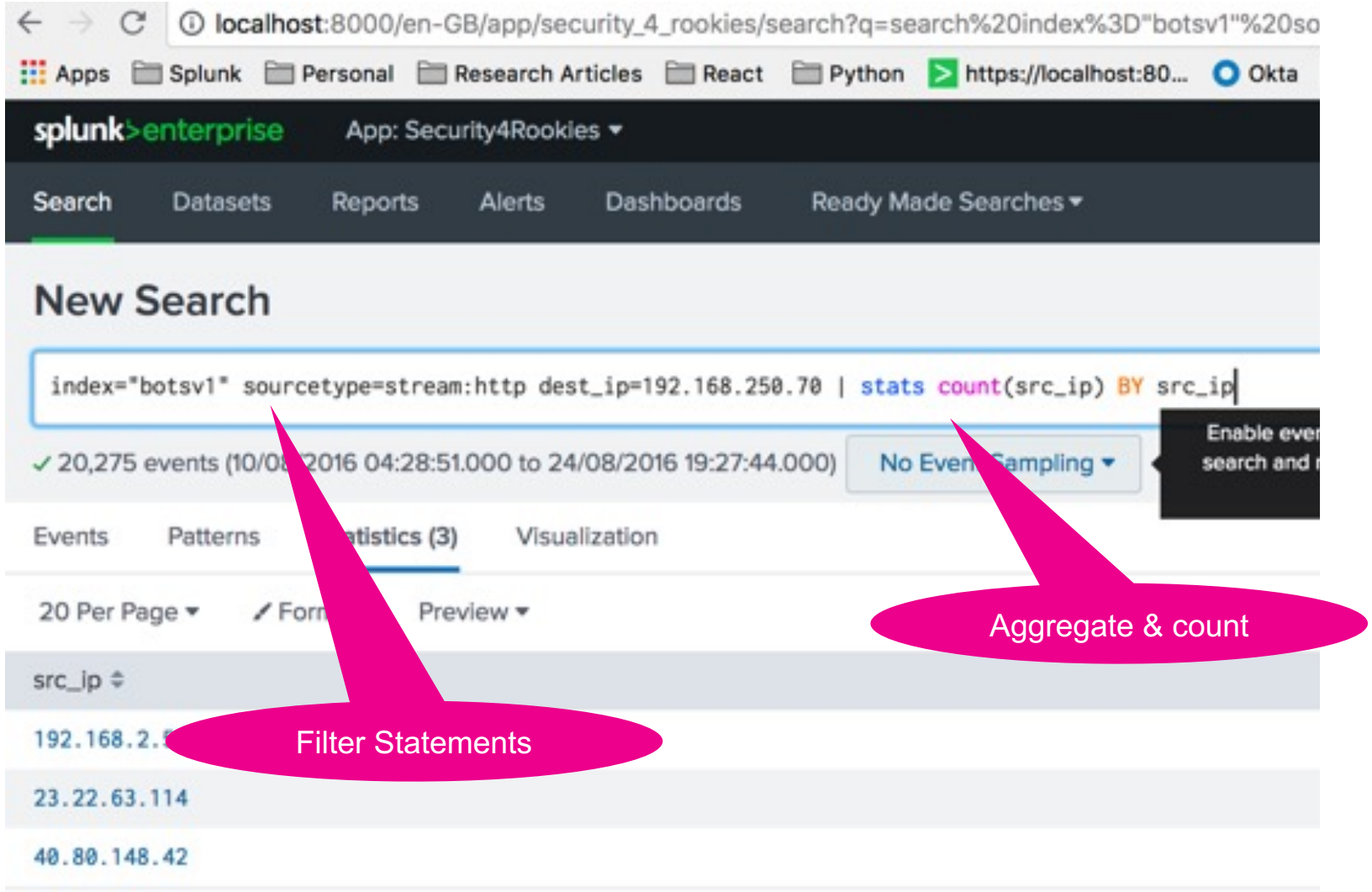
Discovering the attack

Chpt4 – Search 2

Use stats to aggregate

Manual

```
index="botsv1"
sourcetype=stream:http
dest_ip=192.168.250.70
| stats count(src_ip) BY src_ip
```



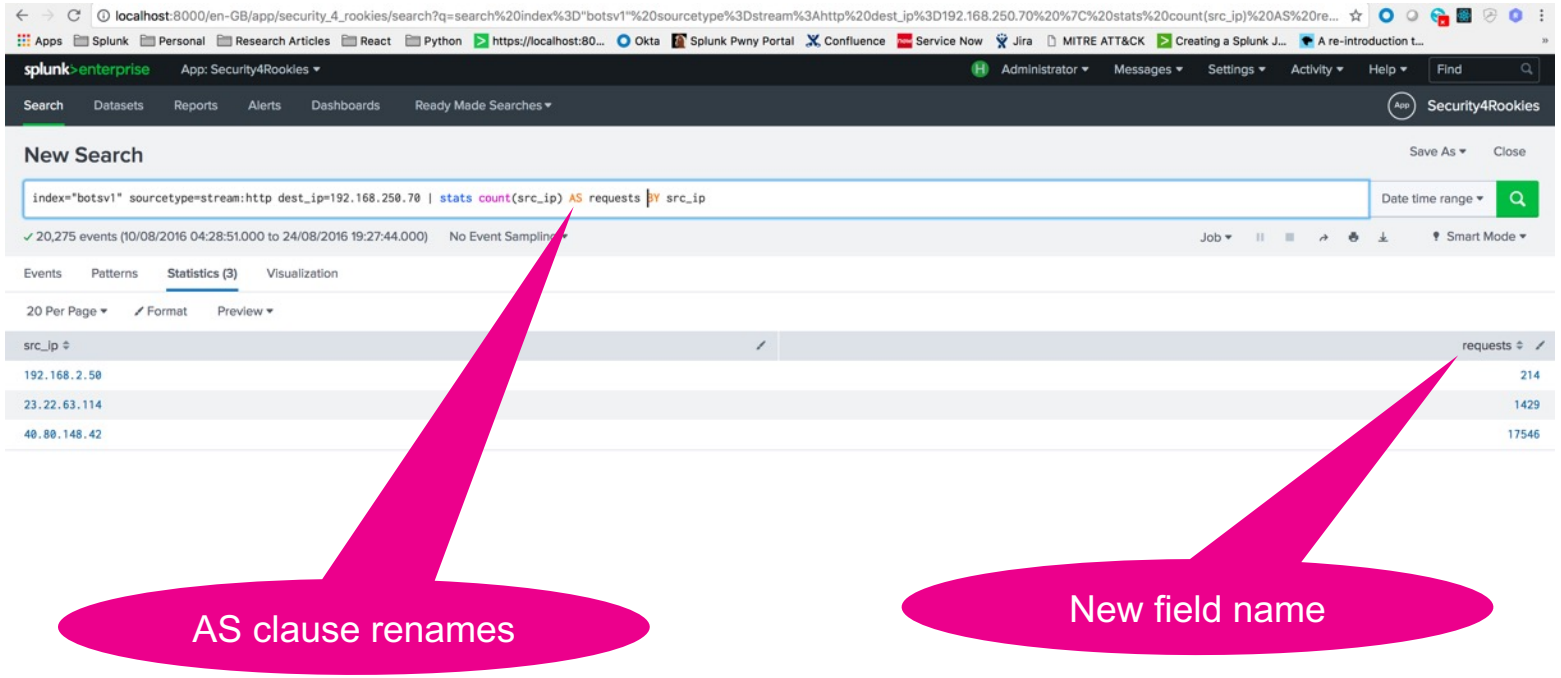
Discovering the attack

Chpt4 – Search 3

Rename fields on the fly

Manual

index="botsv1"
sourcetype=stream:http
dest_ip=192.168.250.70
| stats count(src_ip) AS requests
BY src_ip



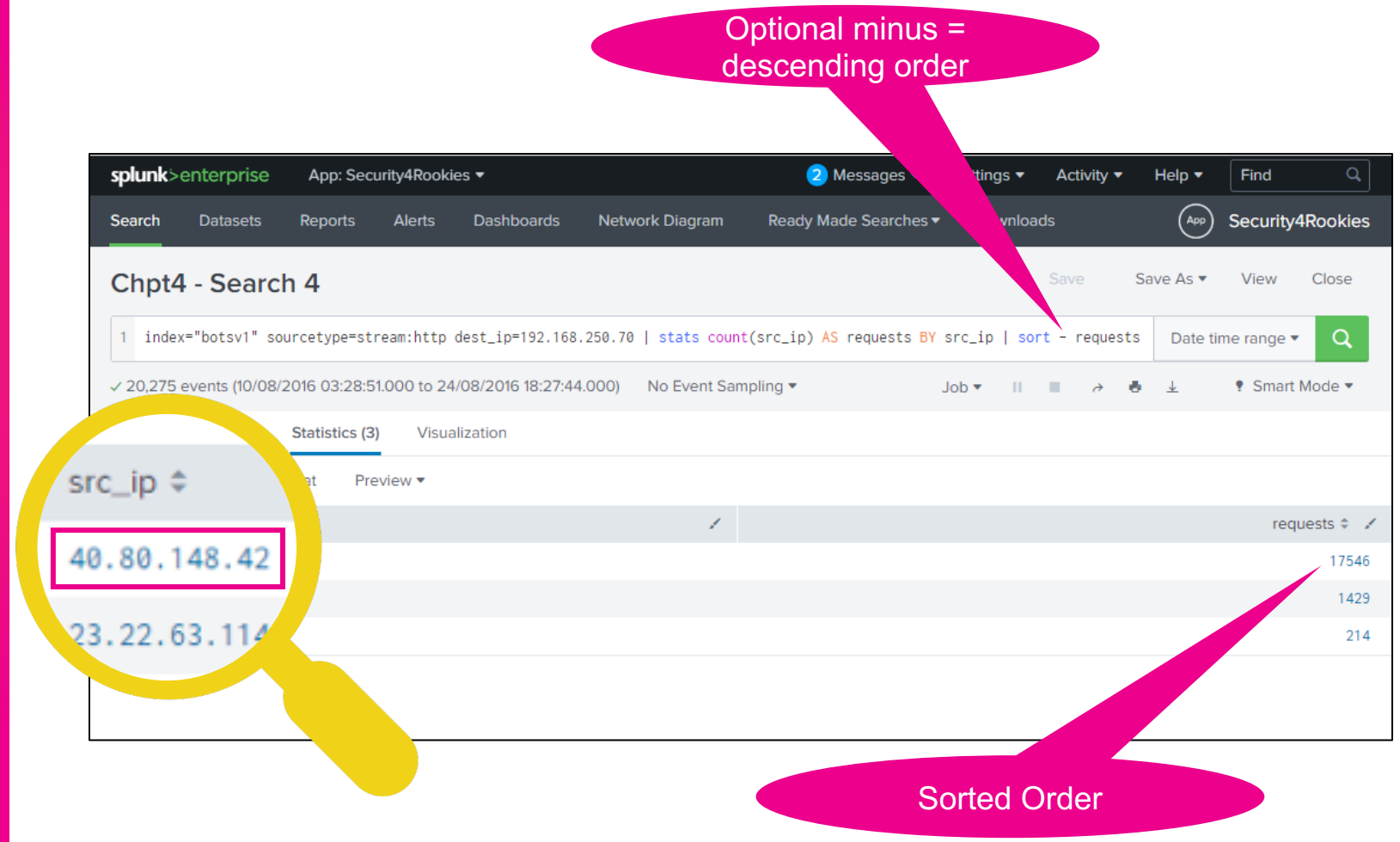
Discovering the attack

Chpt4 – Search 4

Using the sort command

Manual

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



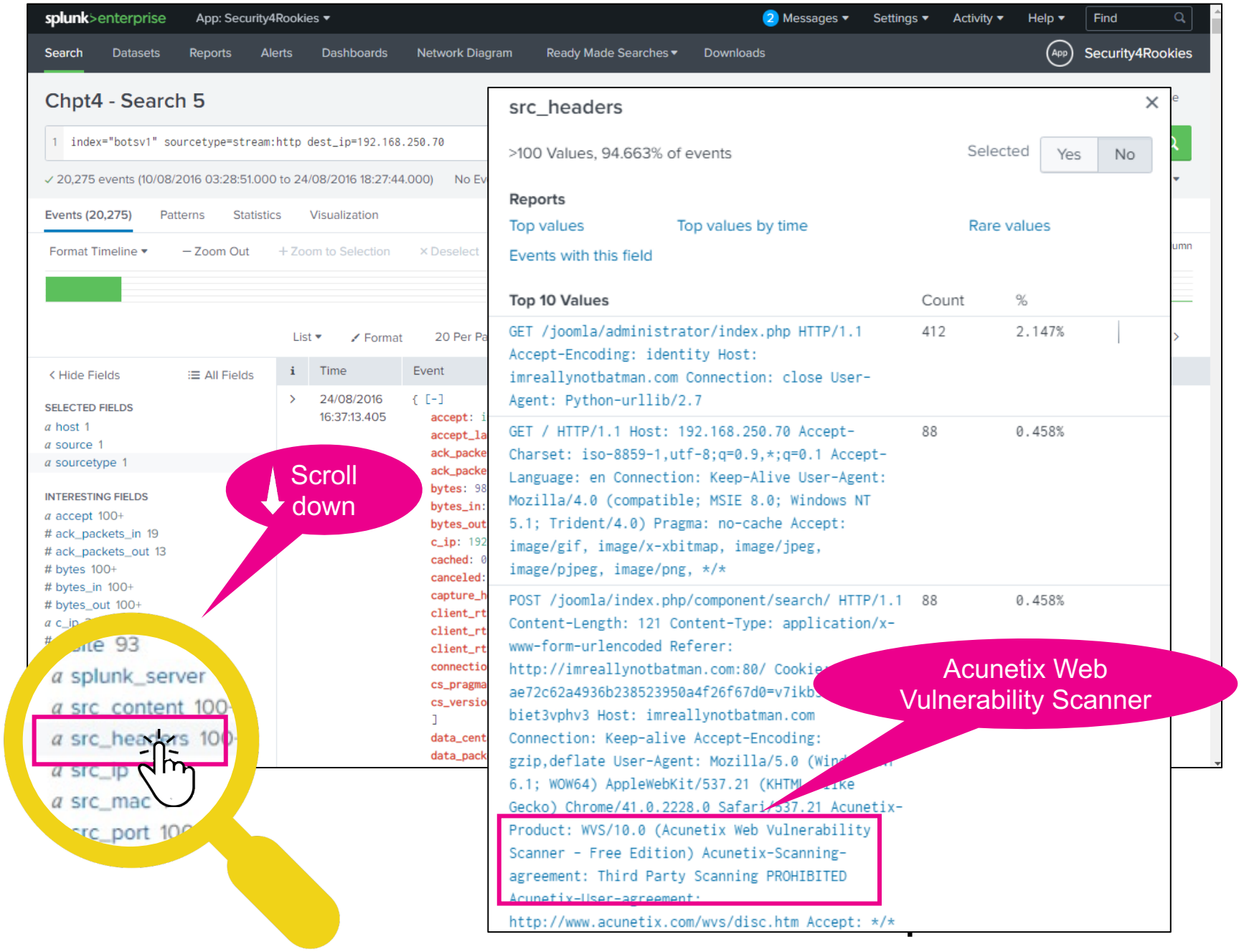
Discovering the attack

Chpt4 – Search 5

Investigating the source headers

Manual

index="botsv1"
sourcetype=stream:http
dest_ip=192.168.250.70



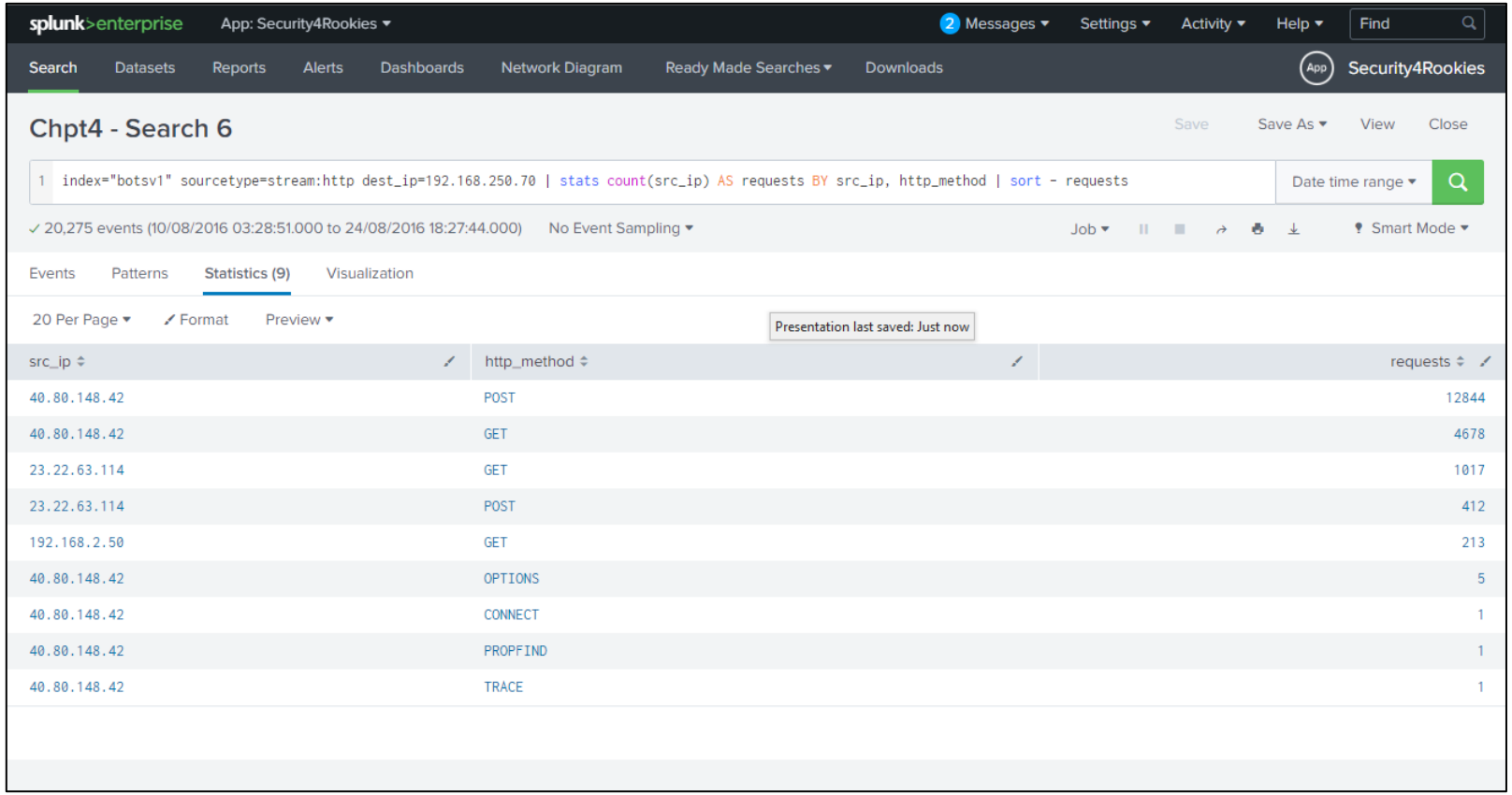
Discovering the attack

Chpt4 – Search 6

Investigating the traffic

Manual

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



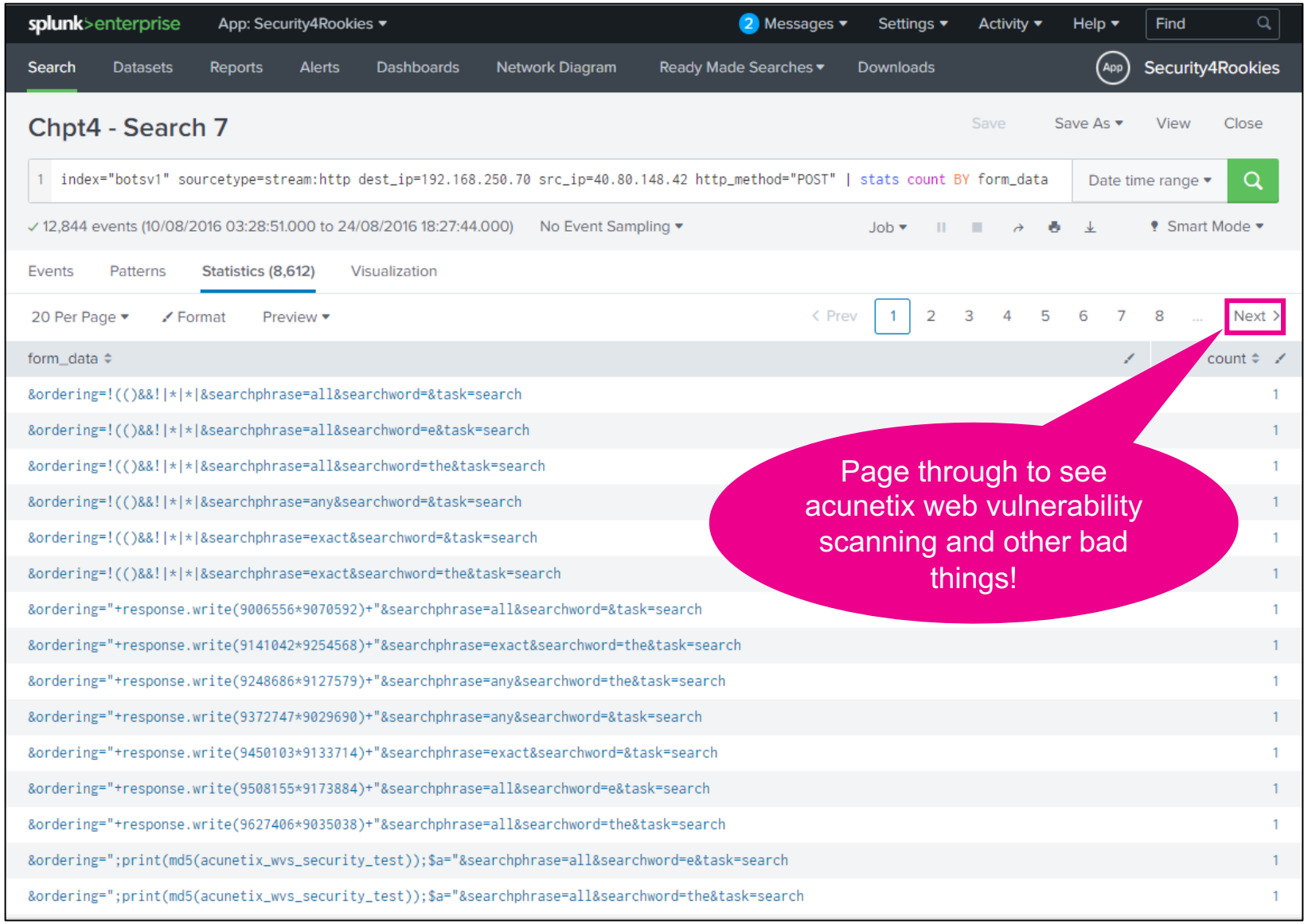
Discovering the attack

Chpt4 – Search 7

Investigating the data being received

Manual

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



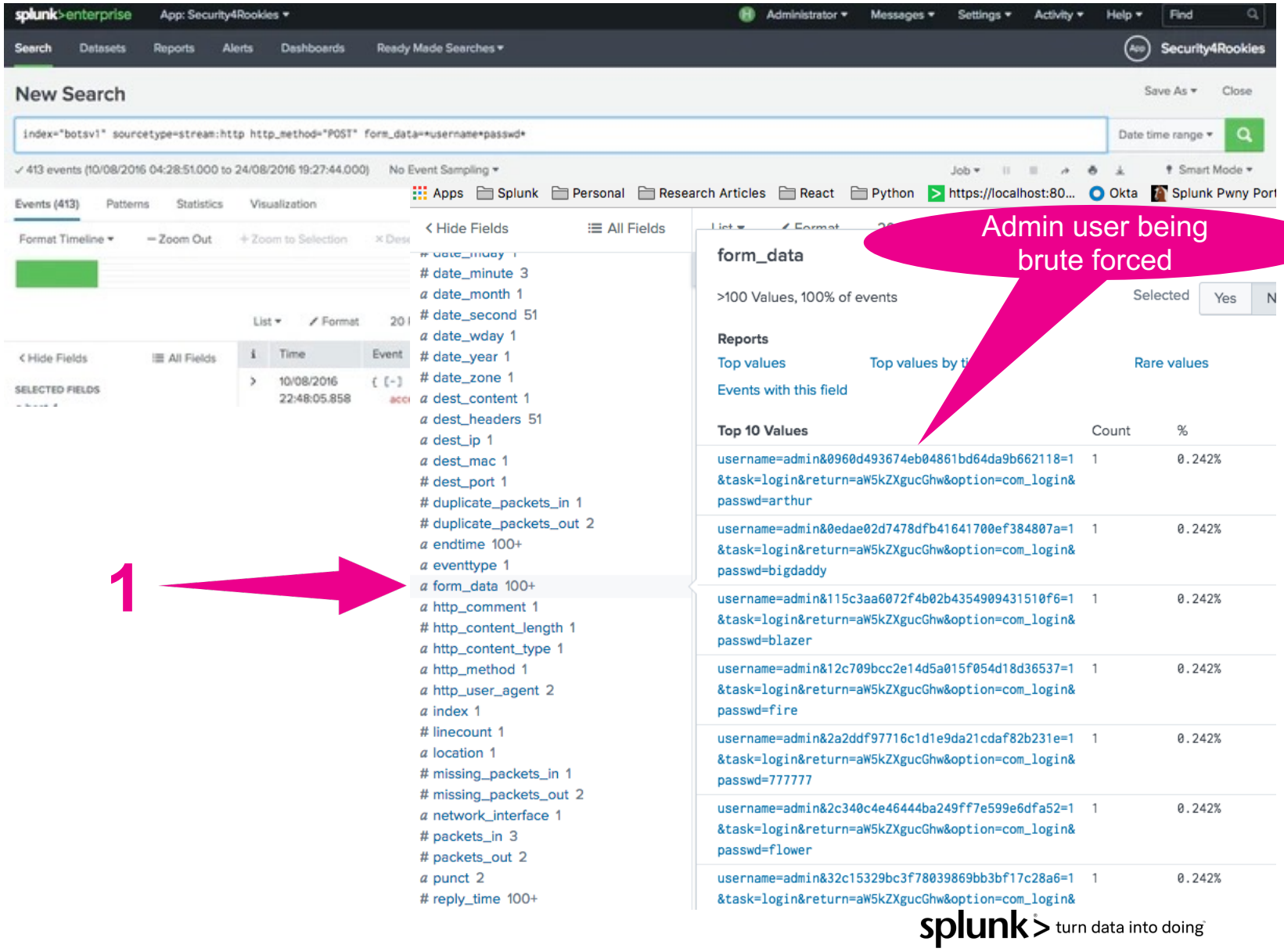
Discovering the attack

Chpt4 – Search 8

Investigating login activity

Manual

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



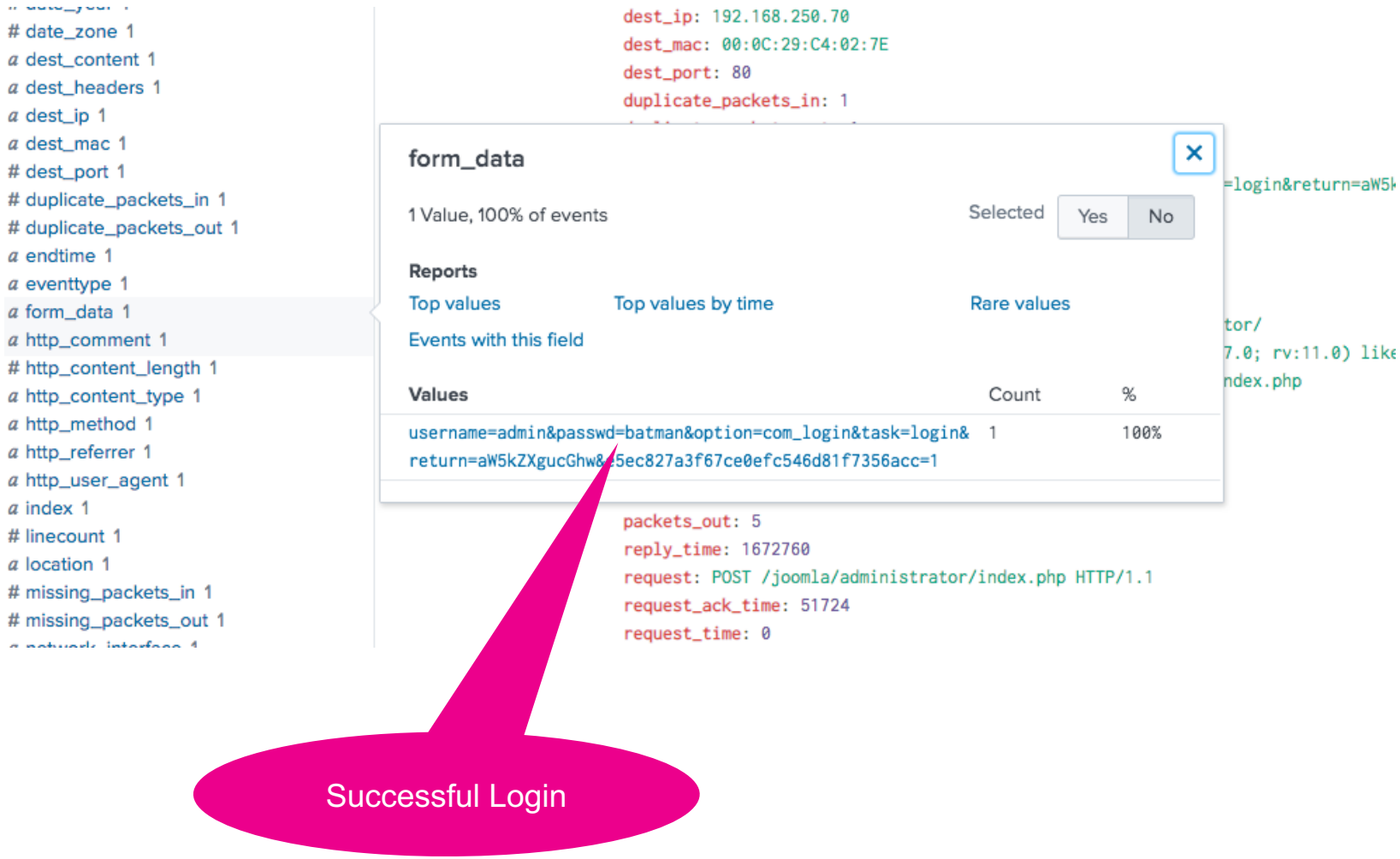
Discovering the attack

Chpt4 – Search 9

Inspecting the login activity

Manual

index="botsv1" sourcetype=stream:http http_method="POST" form_data=*username*passwd* http_user_agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"

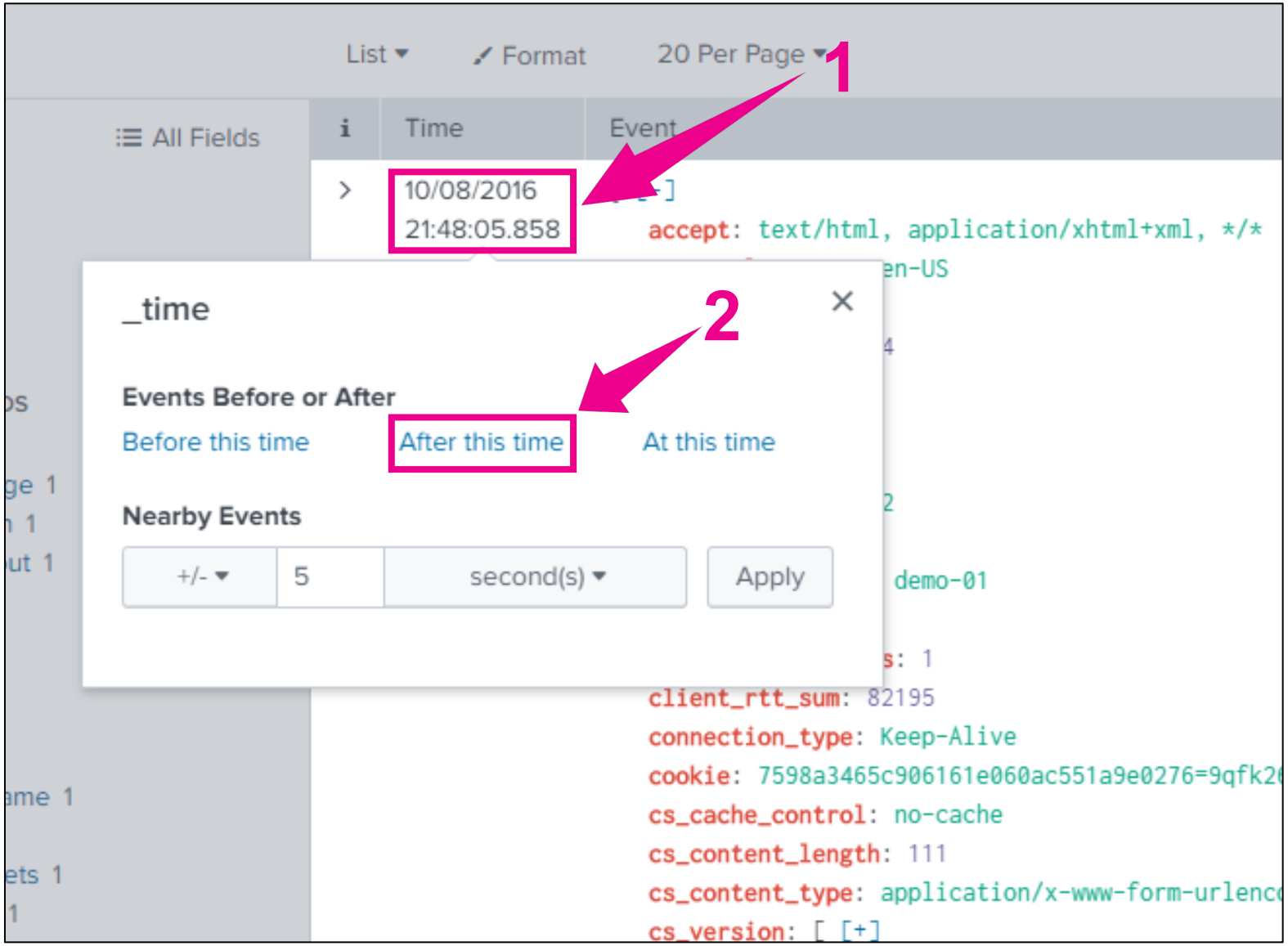


Unauthorized Access ☹

What happened next

Post Exploit

Setting the time range



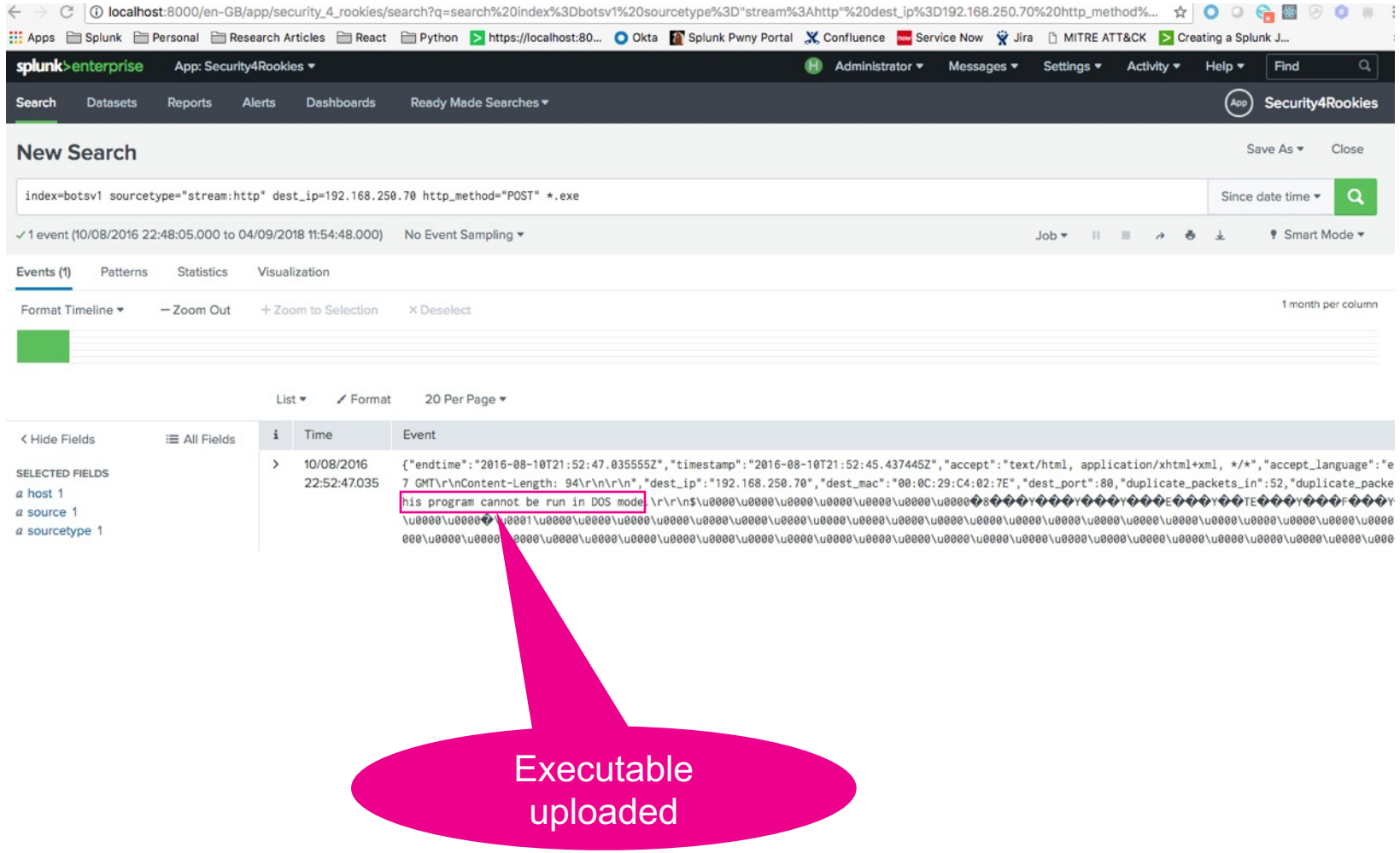
Post Exploit

Chpt5 – Search 1

Looking for a dropper file

Manual

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



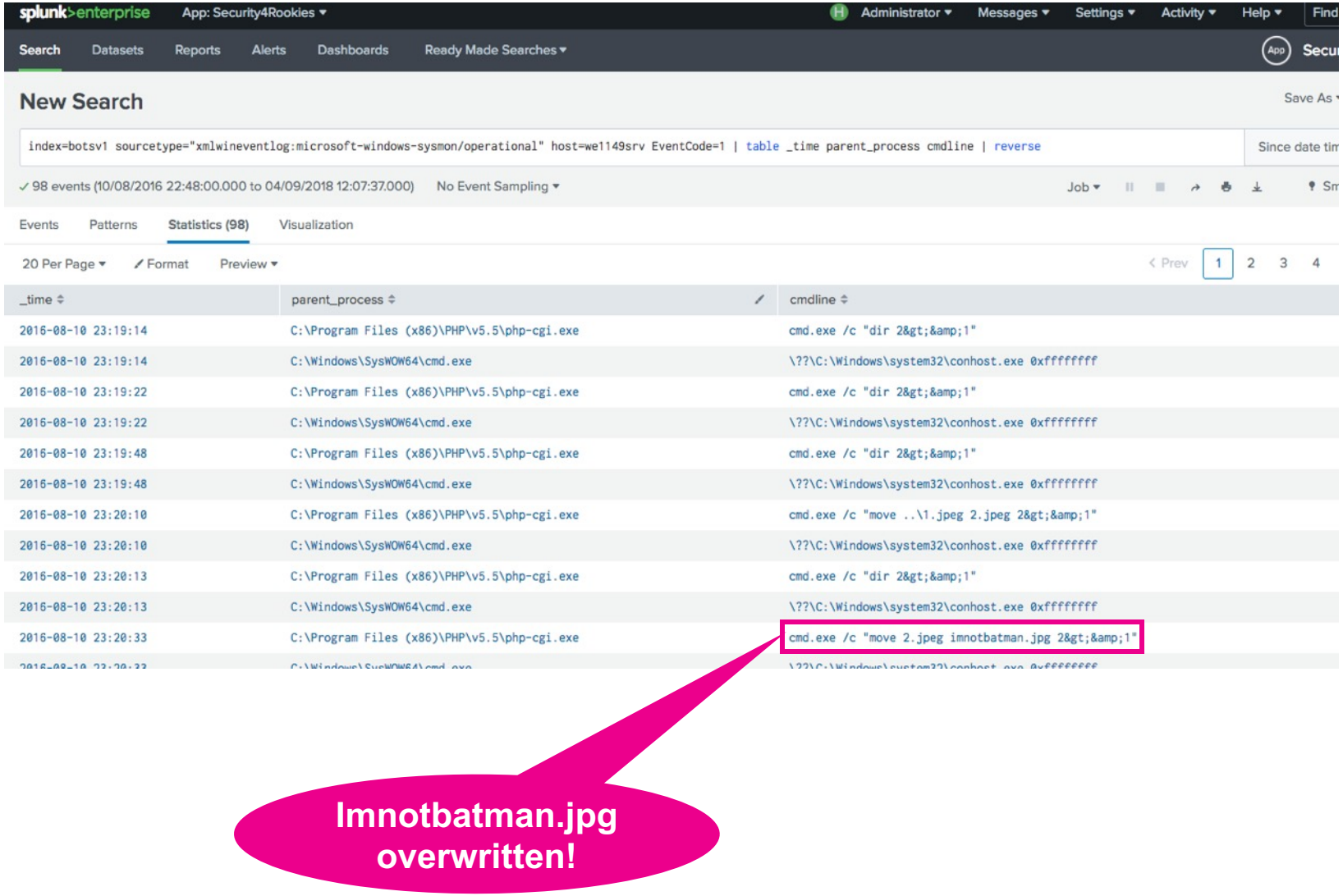
Post Exploit

Chpt5 – Search 2

Investigating Endpoint Processes

Manual

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



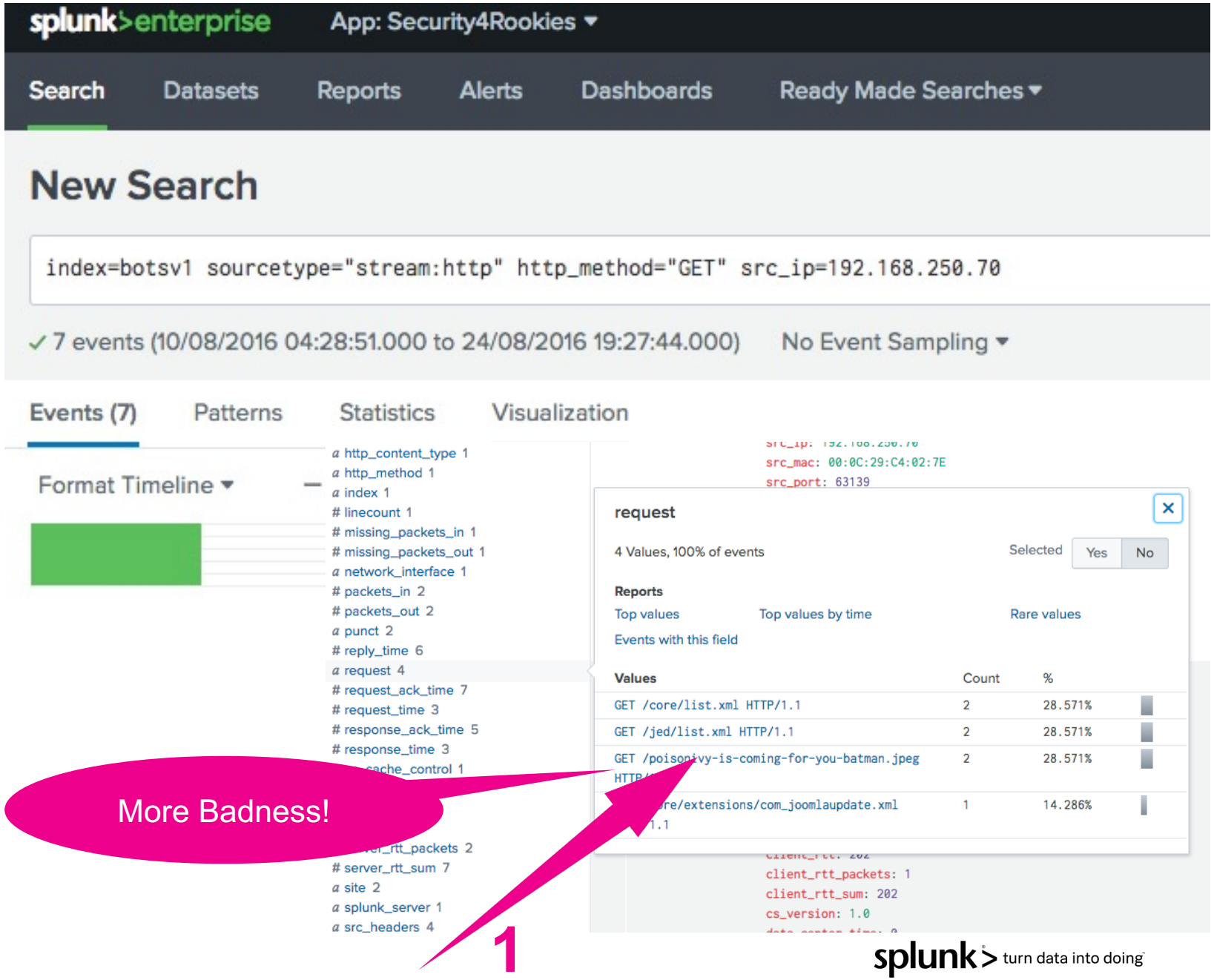
Post Exploit

Chpt5 – Search 3

Investigating Web Server Activity

Manual

index=botsv1
sourcetype="stream:http"
http_method="GET"
src_ip=192.168.250.70



Post Exploit

Chpt5 – Search 3

Investigating Web Server Activity

Manual

index=botsv1
sourcetype="stream:http"
http_method="GET"
src_ip=192.168.250.70

Dashboards

My Manager wants them now! - OK

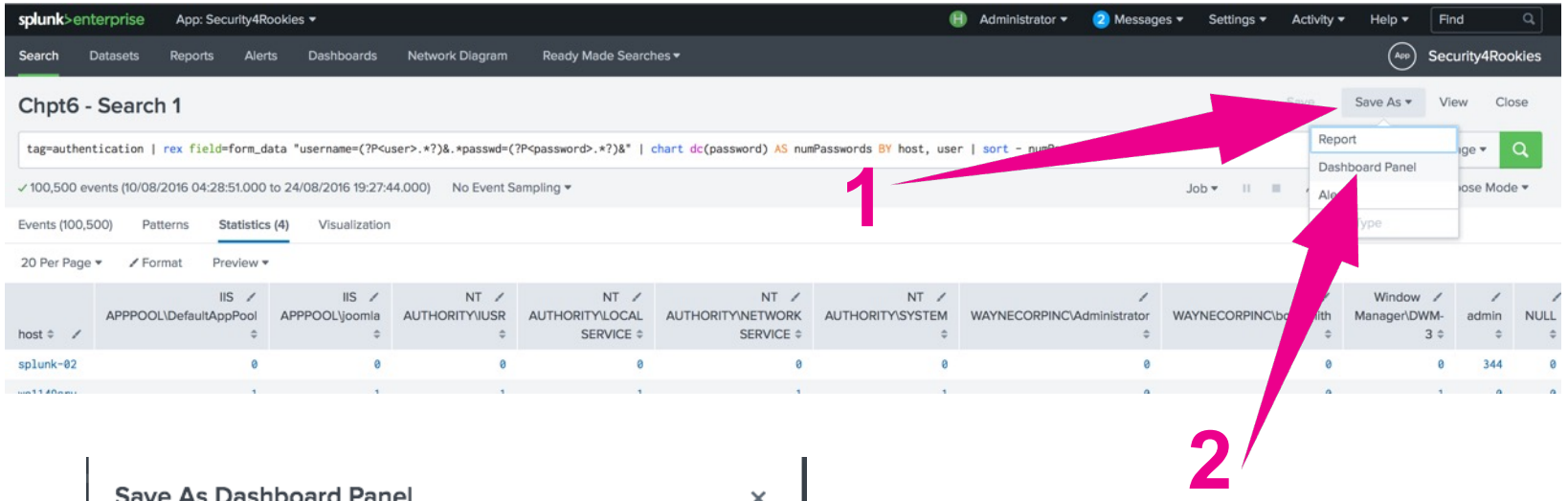
Dashboards

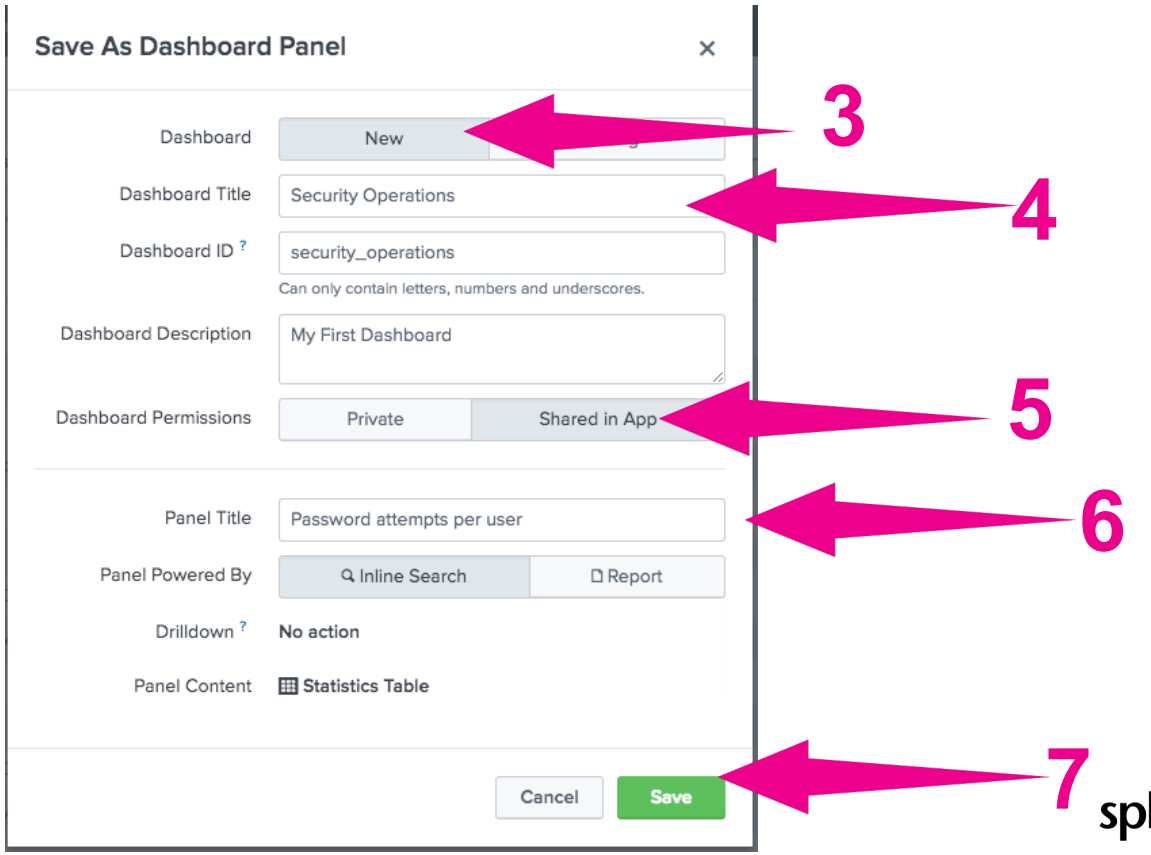
Chpt6 – Search 1

Brute Force Activity into our web site

Manual

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





splunk> turn data into doing

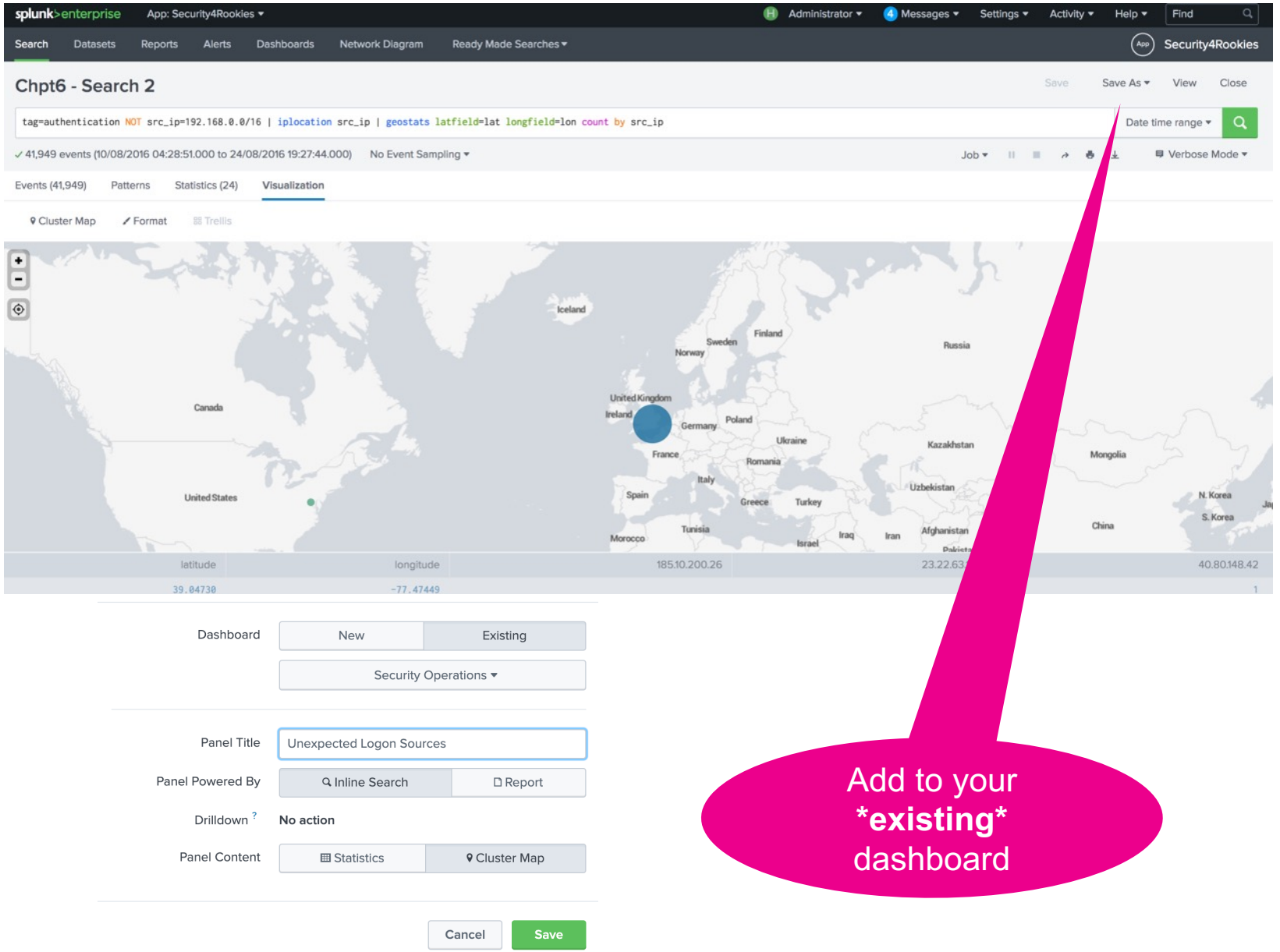
Dashboards

Chpt6 – Search 2

Unexpected Logon Sources

Manual

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



Add to your ***existing*** dashboard

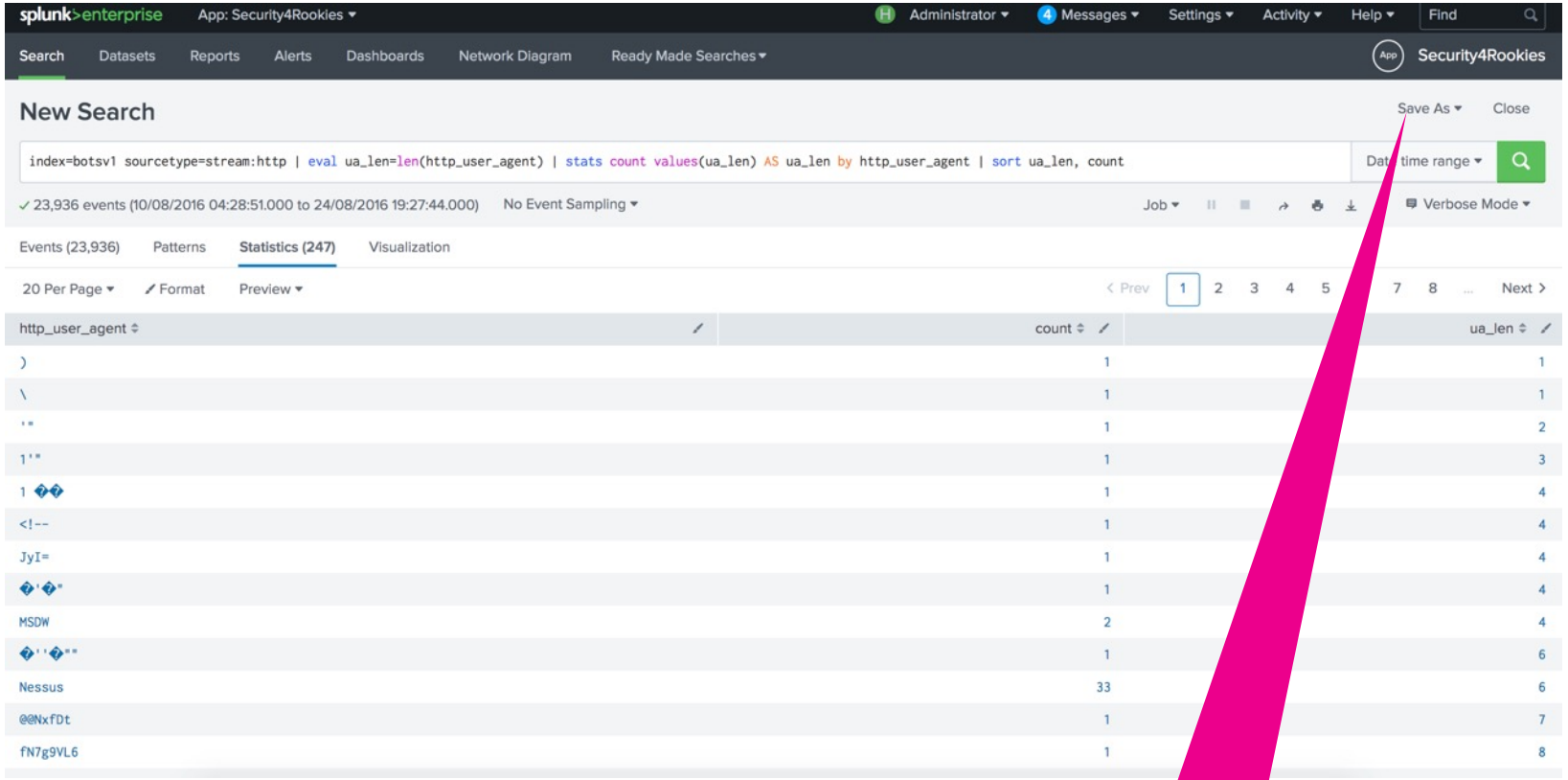
Dashboards

Chpt6 – Search 3

Analyzing user agent lengths

Manual

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



Add to your existing dashboard

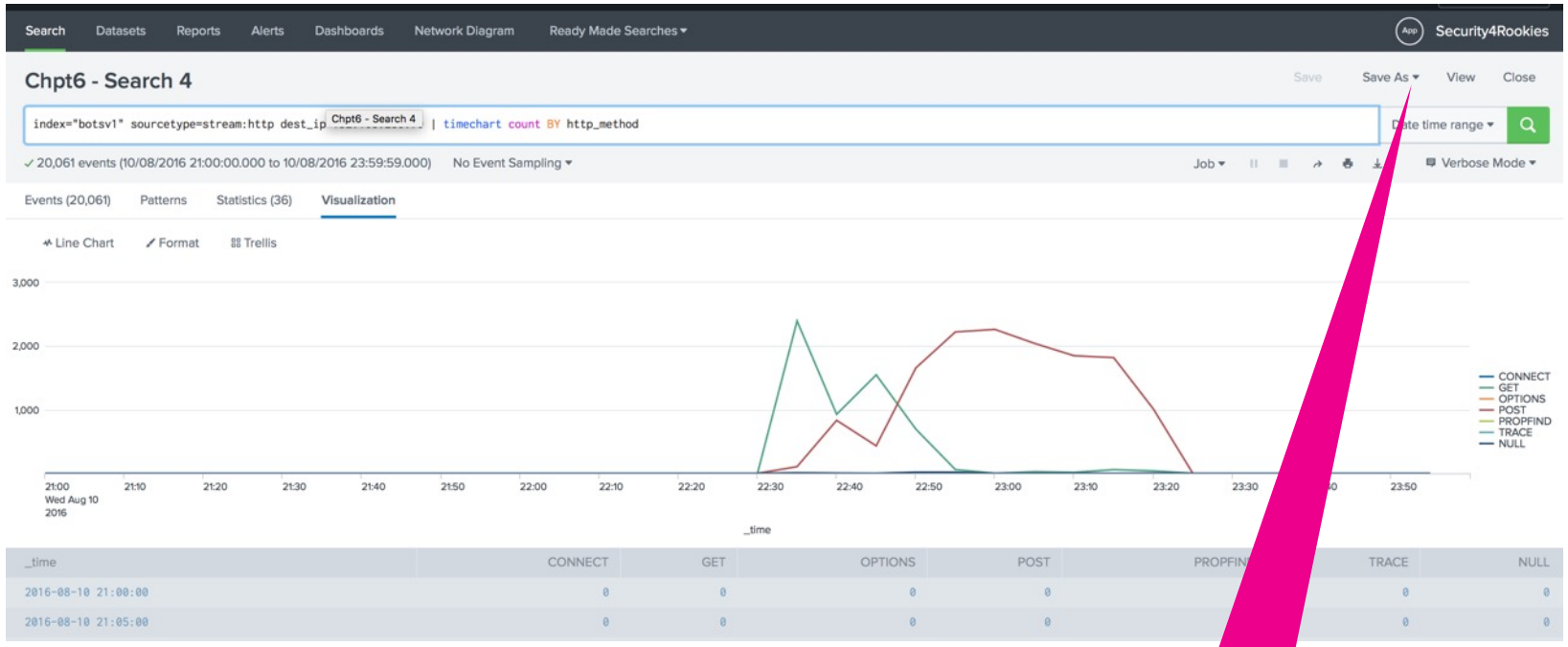
Dashboards

Chpt6 – Search 4

Web Traffic by Method

Manual

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



Add to your existing dashboard

splunk> turn data into doing

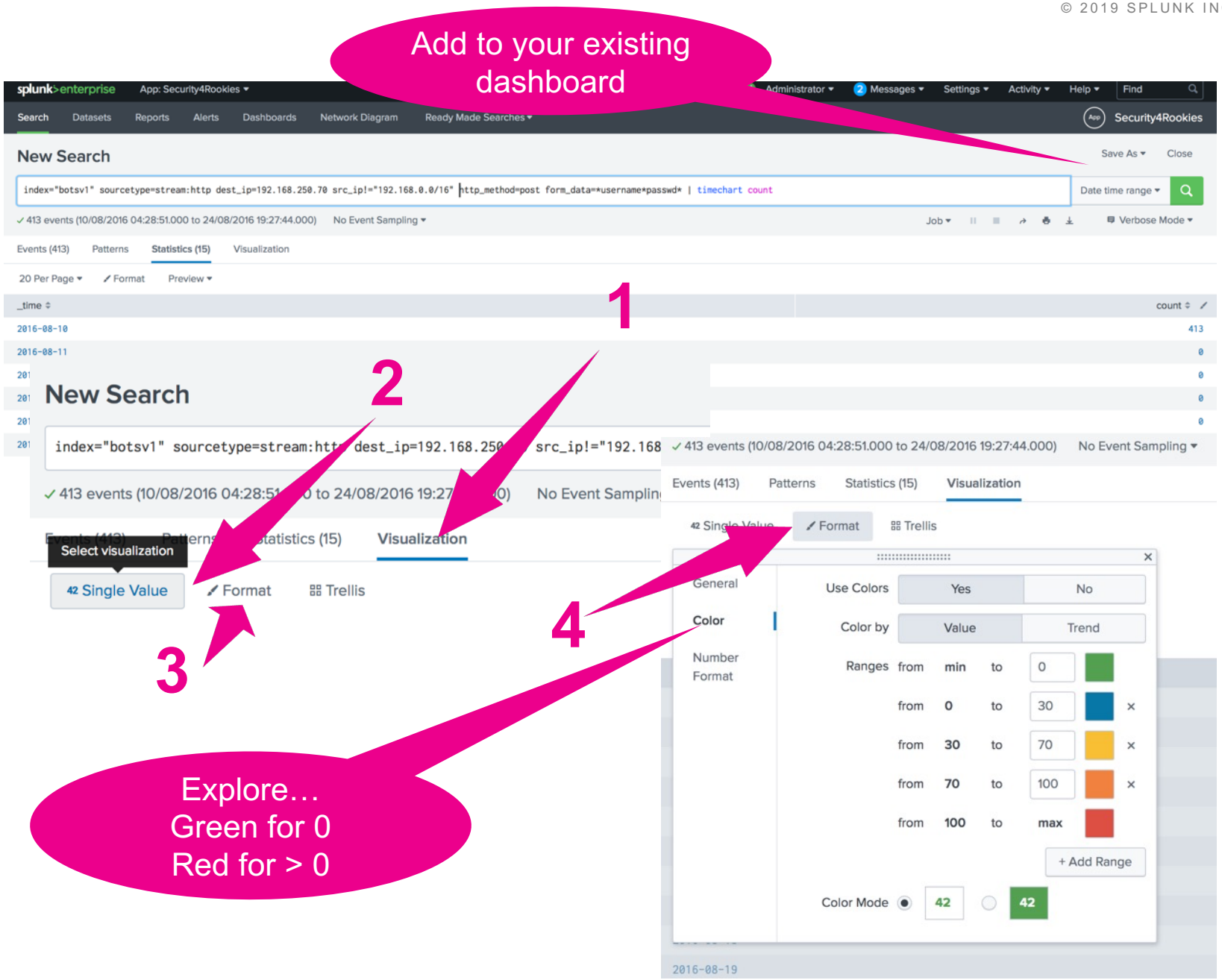
Dashboards

Chpt6 – Search 5

Attempted website logons by external IPs

Manual

```
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> turn data into doing

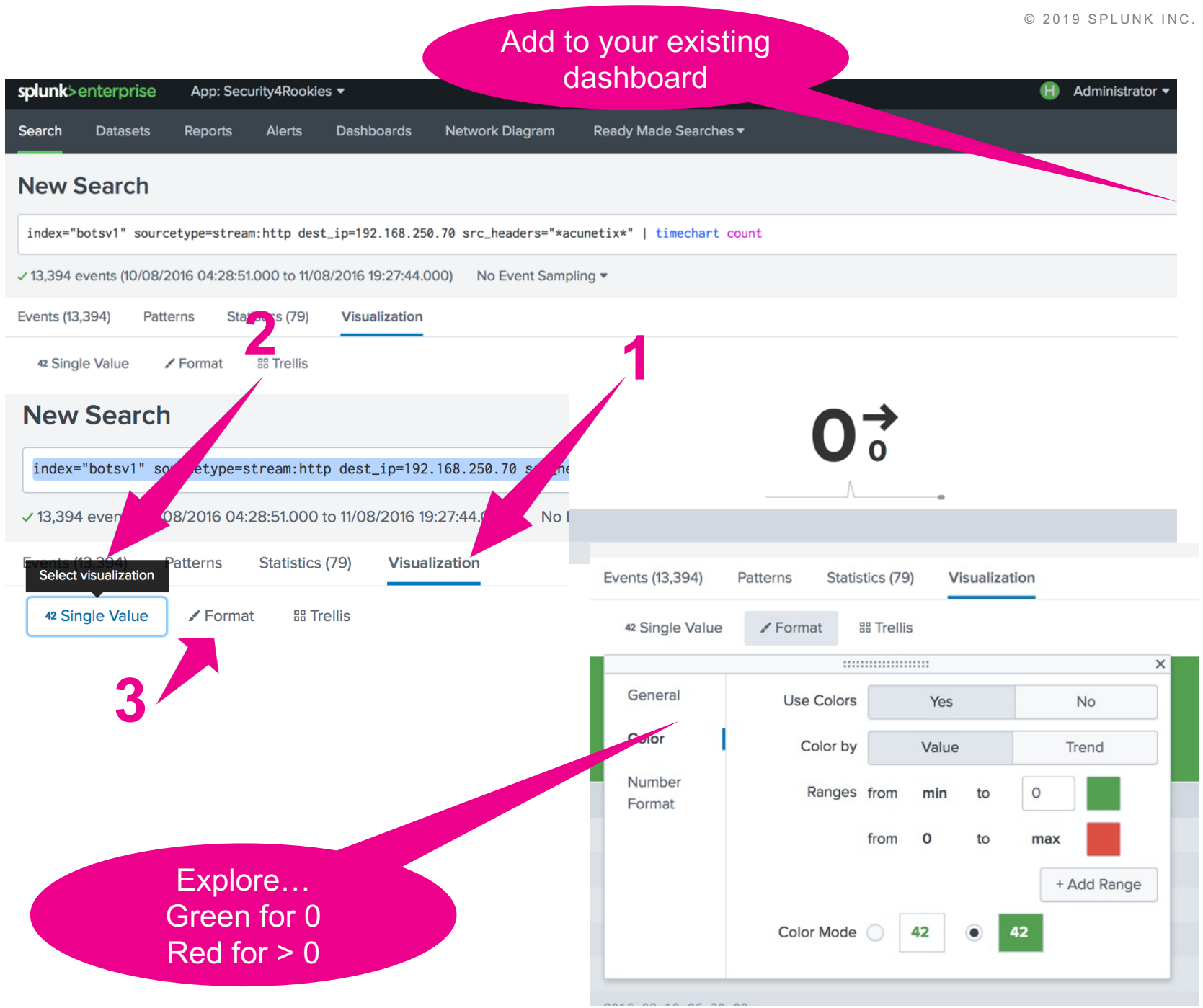
Dashboards

Chpt6 – Search 6

Scanning Activity by known vulnerability scanners

Manual

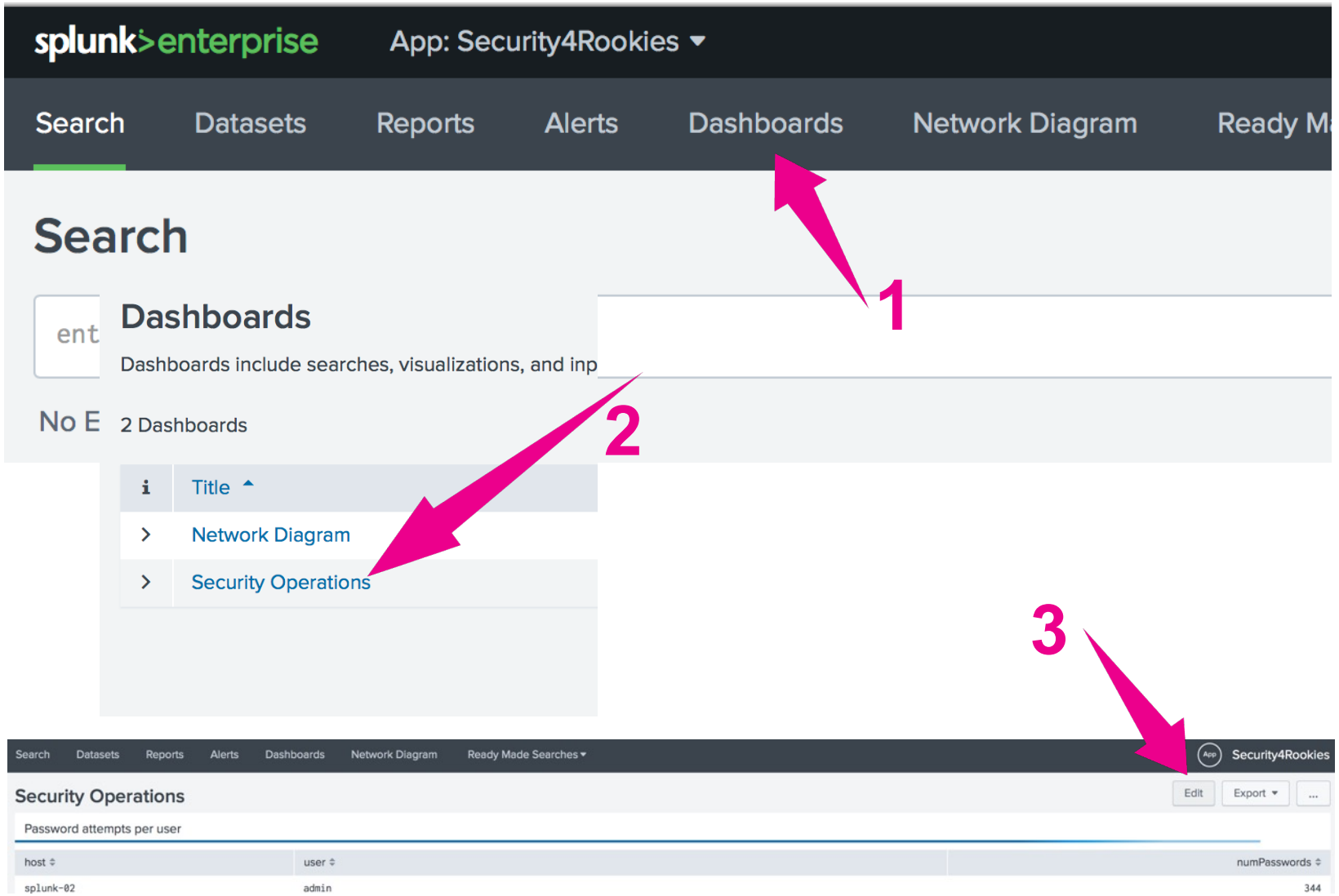
```
index="botsv1"
sourcetype=stream:http
dest_ip=192.168.250.70
src_headers="*acunetix*" |
timechart count
```



Dashboards

Visualizations

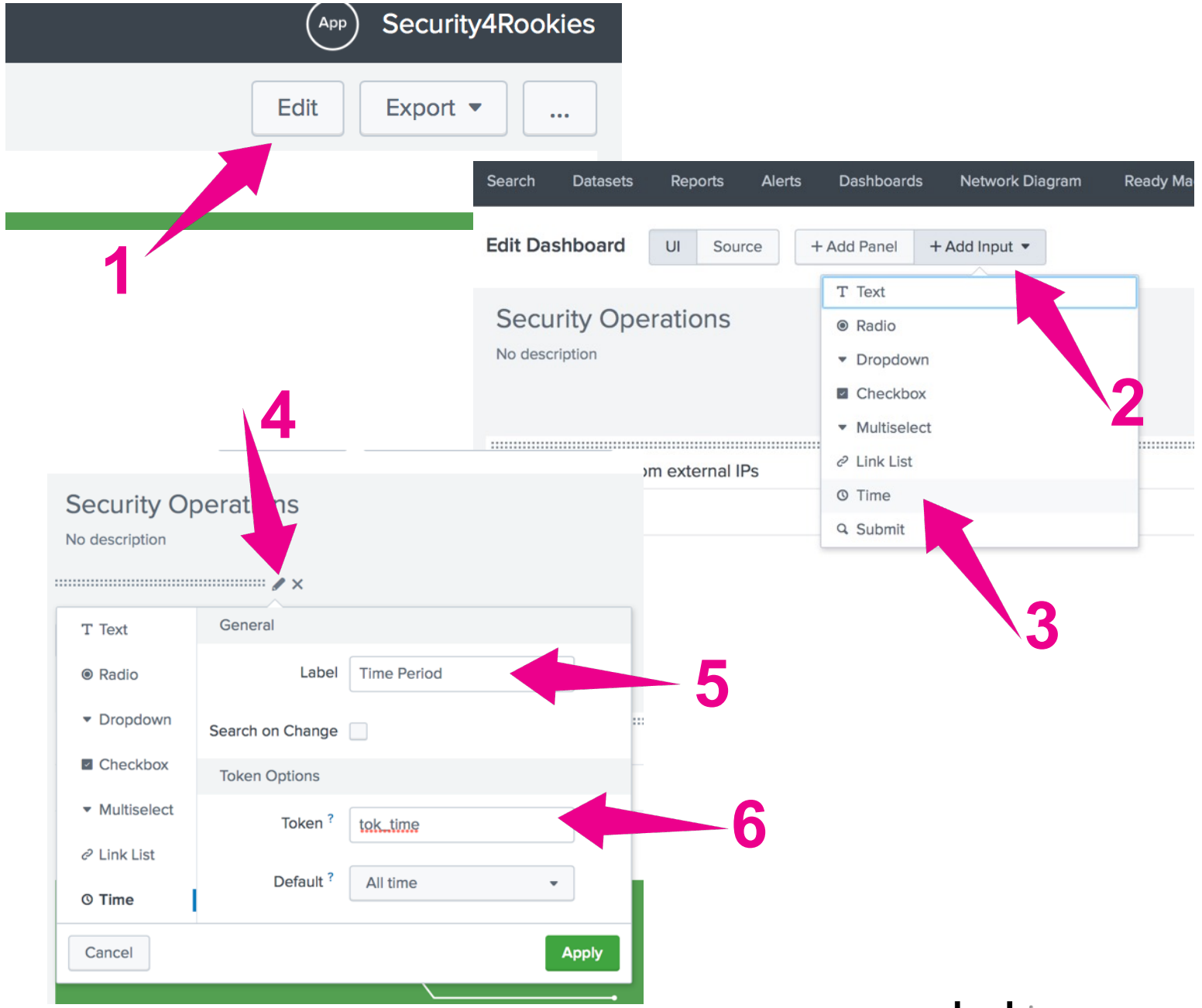
Interactive



Dashboards

Visualizations

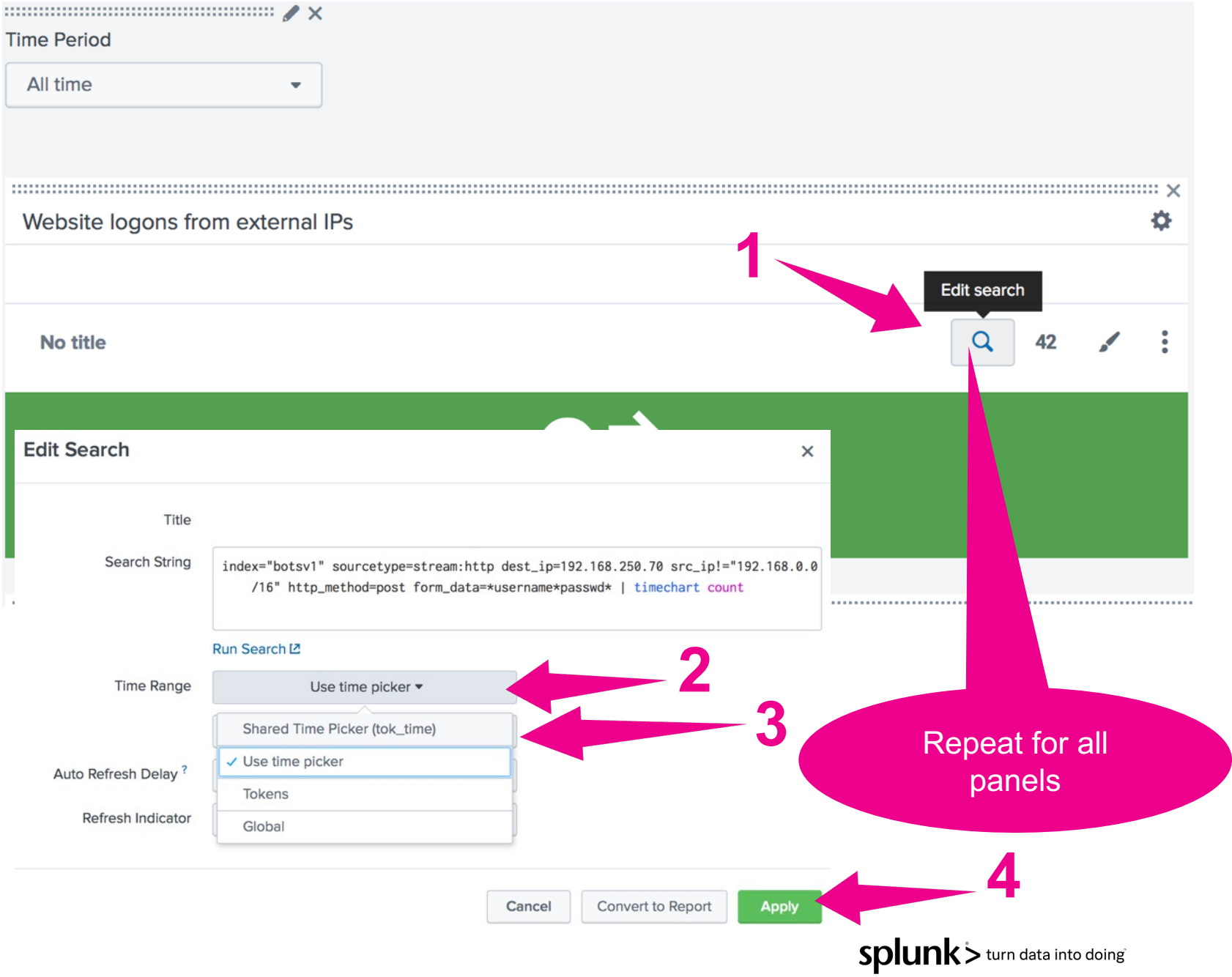
Add time selector



Dashboards

Visualizations

Make panels react

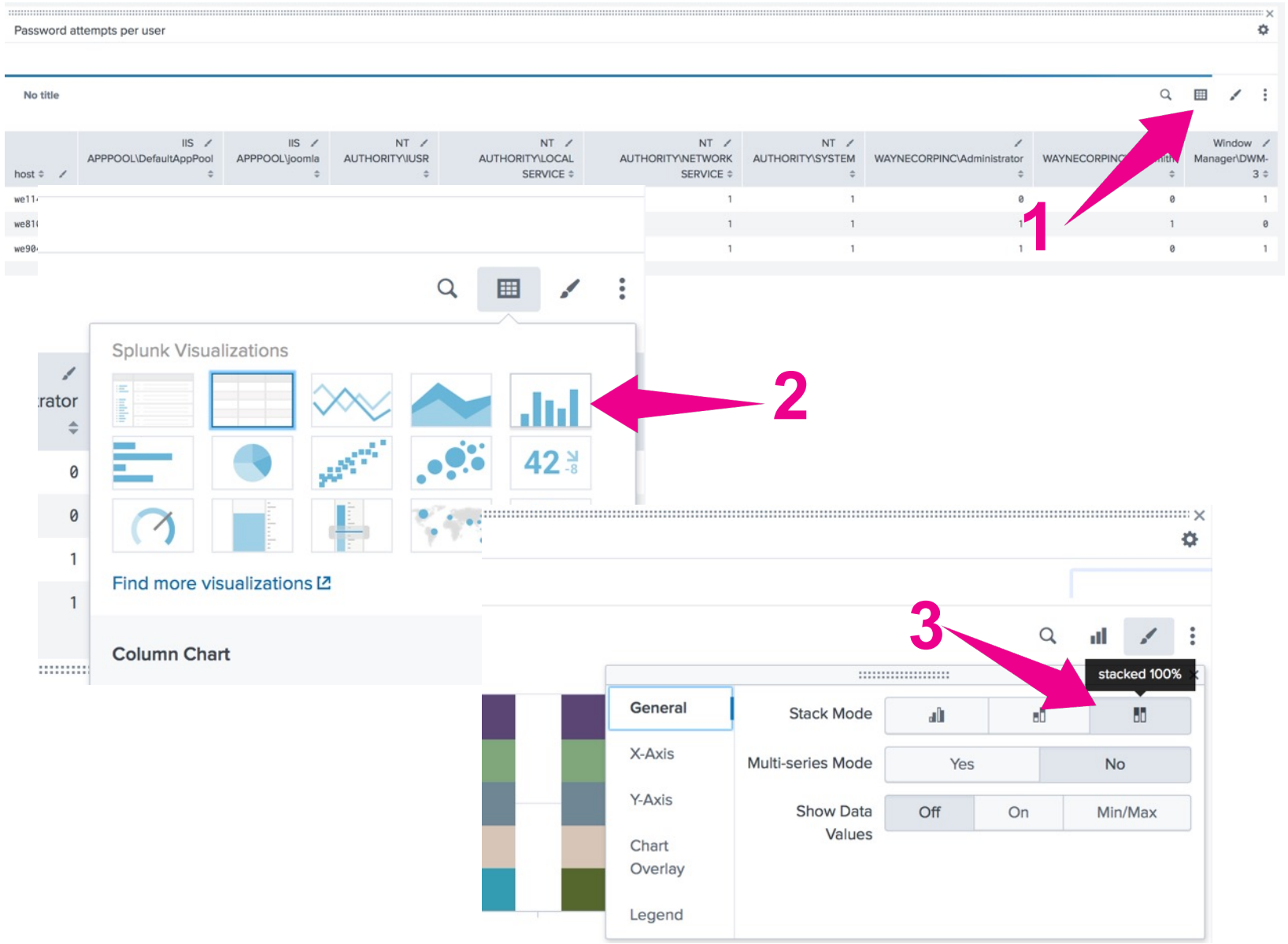


splunk> turn data into doing

Dashboards

Visualizations

Changing Visualization Type



Dashboards

Visualizations

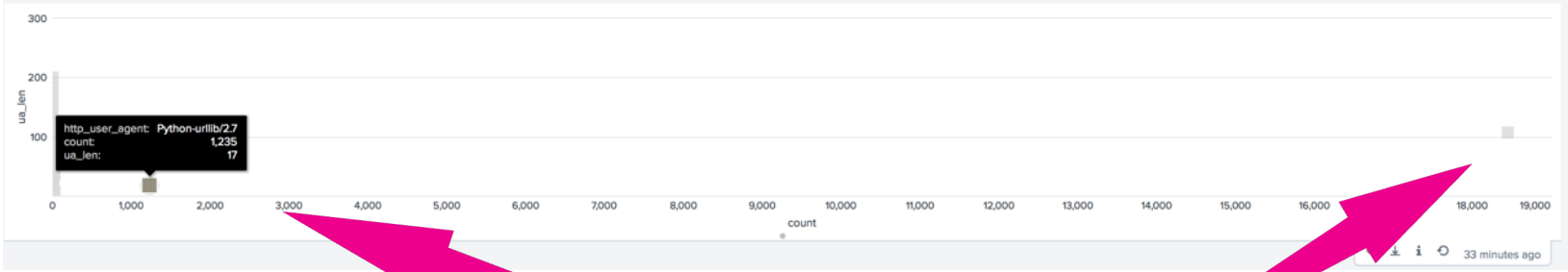
Bonus Challenge

Change http_user_agent panel to a scatter chart

http_user_agent	count	ua_len
)	1	1
\	1	1
'"	1	2
1'"	1	3
1 ▯▯	1	4
<!--	1	4
JyI=	1	4
▯'▯"	1	4
MSDW	2	4
▯''▯""	1	6

« prev 1 2 3 4 5 6 7 8 9 10 next »

YUK! – Wrong type of vis for the data!



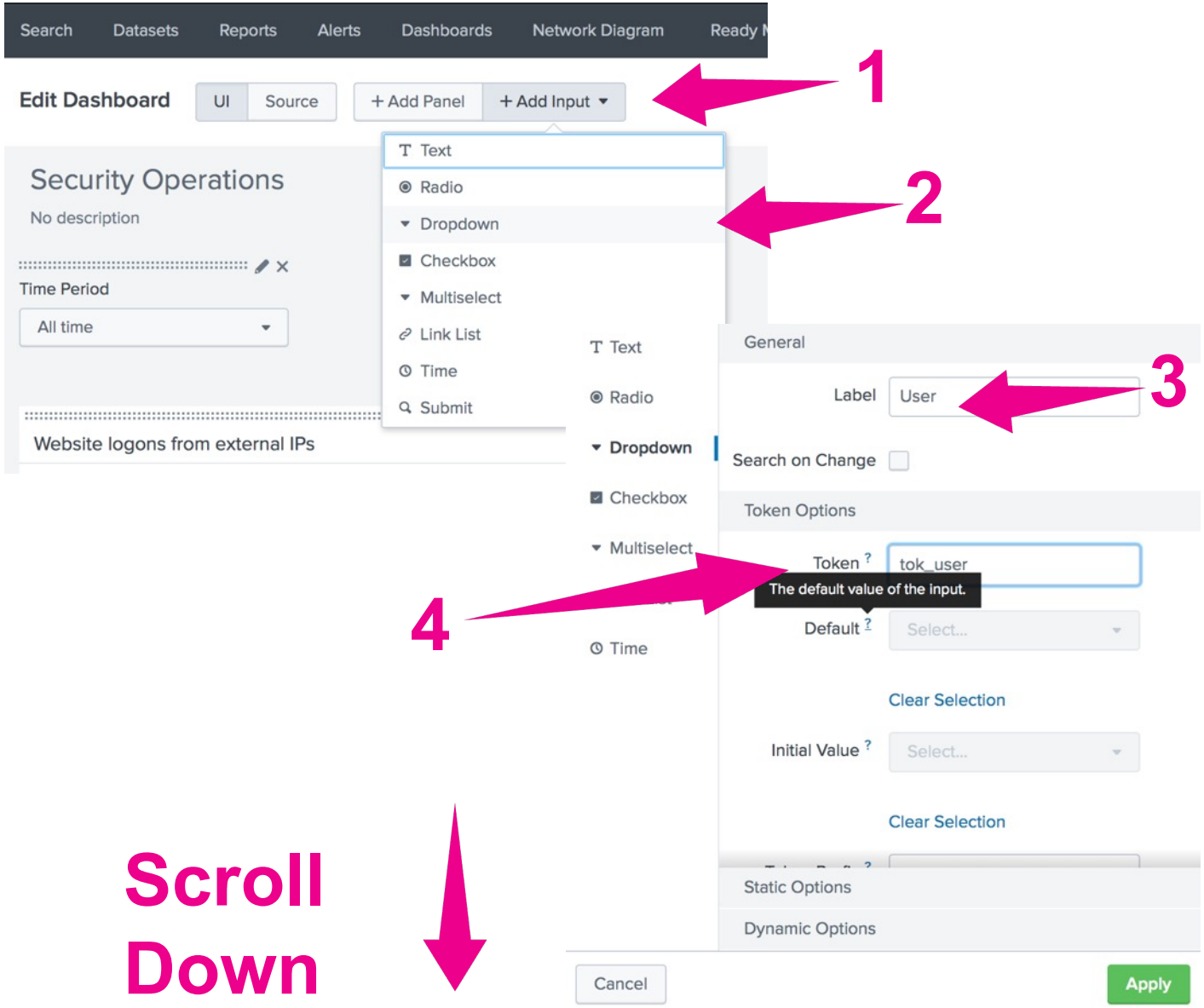
Rare features stand out with good visualizations

splunk> turn data into doing

Dashboards

Visualizations

Interactive Filtering

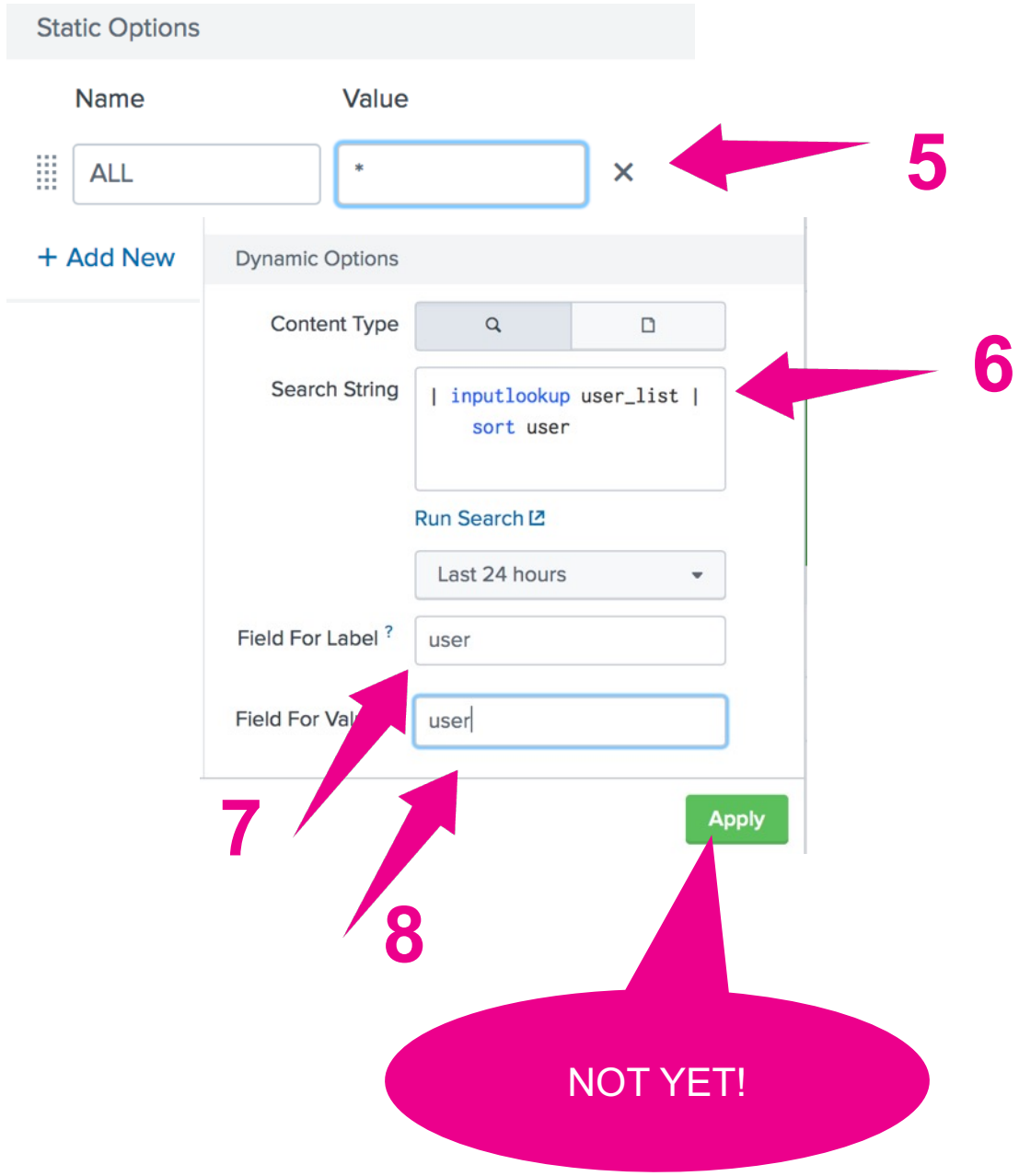


splunk> turn data into doing

Dashboards

Visualizations

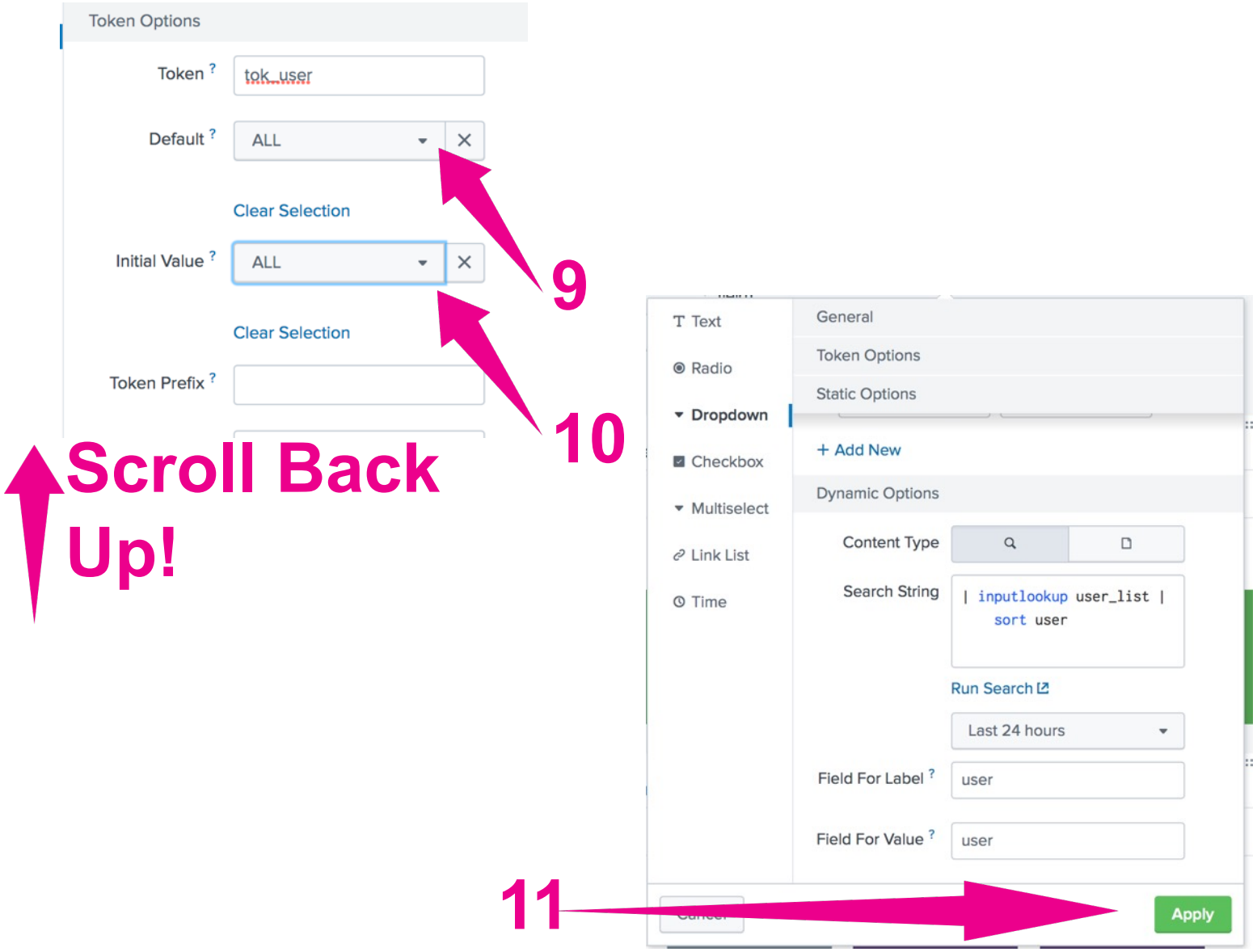
Continued



Dashboards

Visualizations

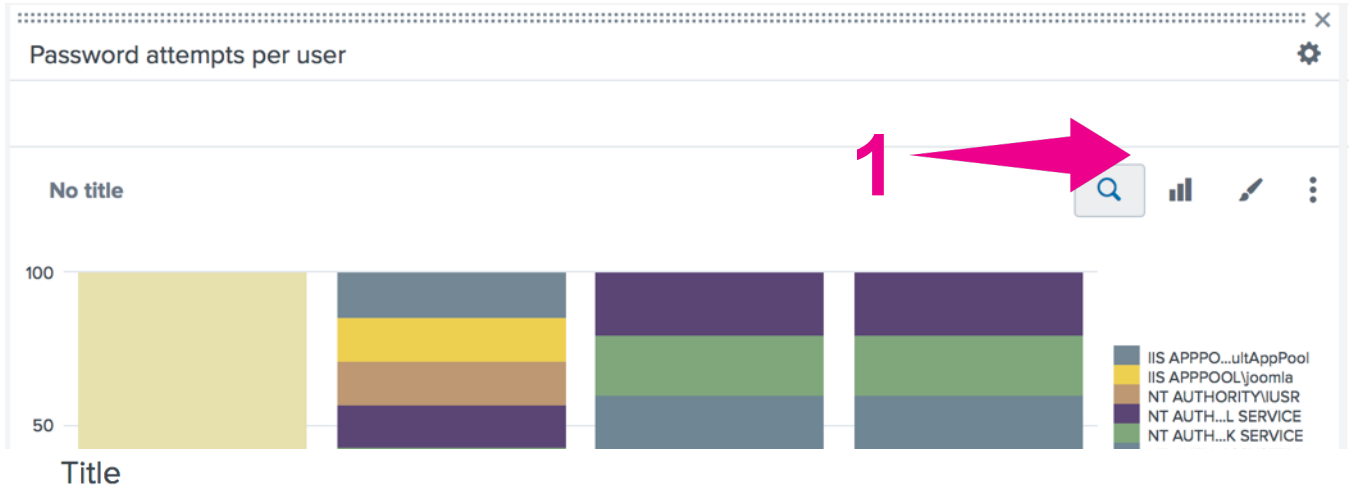
Continued



Dashboards

Visualizations

Substitute tokens into a dashboard search



Search String

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

Run Search

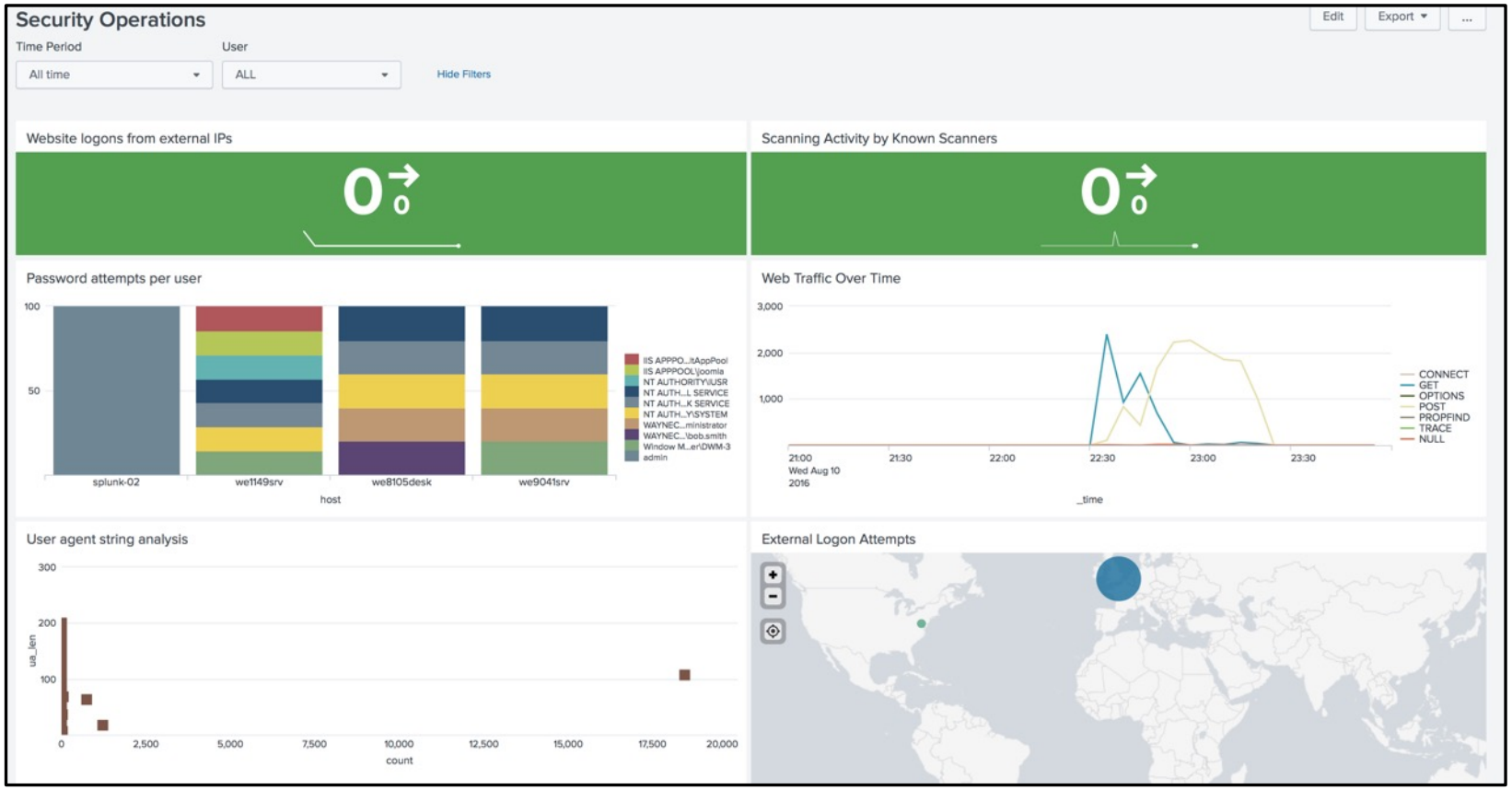
ADD
“search user=tok_user |”

splunk> turn data into doing

Dashboards

Dashboard Hero

And….. Breathe!



splunk> turn data into doing

Splunk Resources

Resources

Helpful ‘Stuff’

1) **Splunk command ‘cheat sheet’**
   https://www.splunk.com/pdfs/solution-guides/splunk-quick-reference-guide.pdf

2) **App for Security Monitoring**
   https://splunkbase.splunk.com/app/4131/

3) **App for Security Essentials**
   https://splunkbase.splunk.com/app/3435/

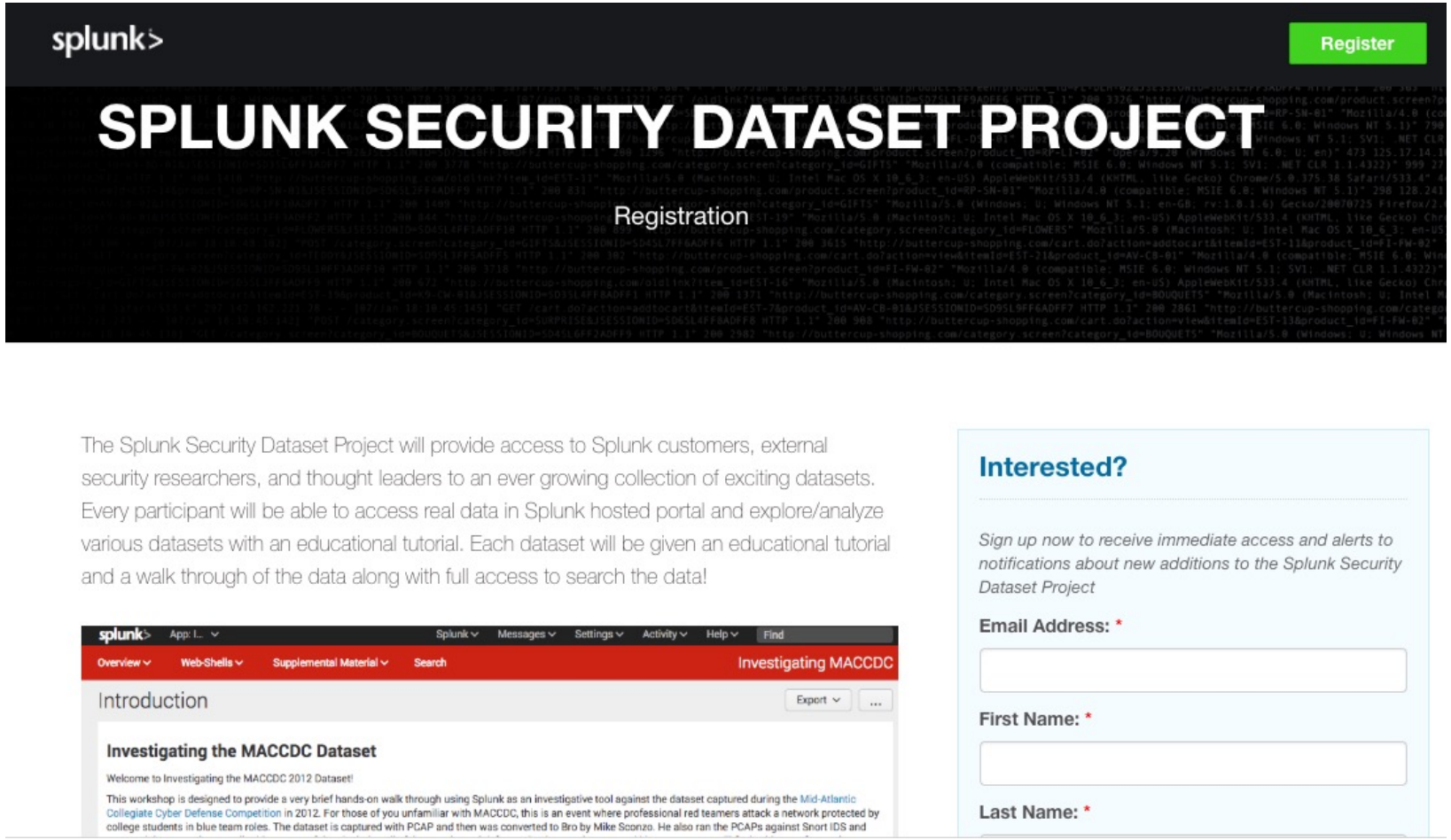
4) **Splunk Accredited Education**
   https://www.splunk.com/view/SP-CAAAH9U

5) **Free Splunk Education!**
   https://www.splunk.com/en_us/training/free-courses/splunk-fundamentals-1.html

6) **Splunk Documentation**
   http://docs.splunk.com/

Need more inspiration?

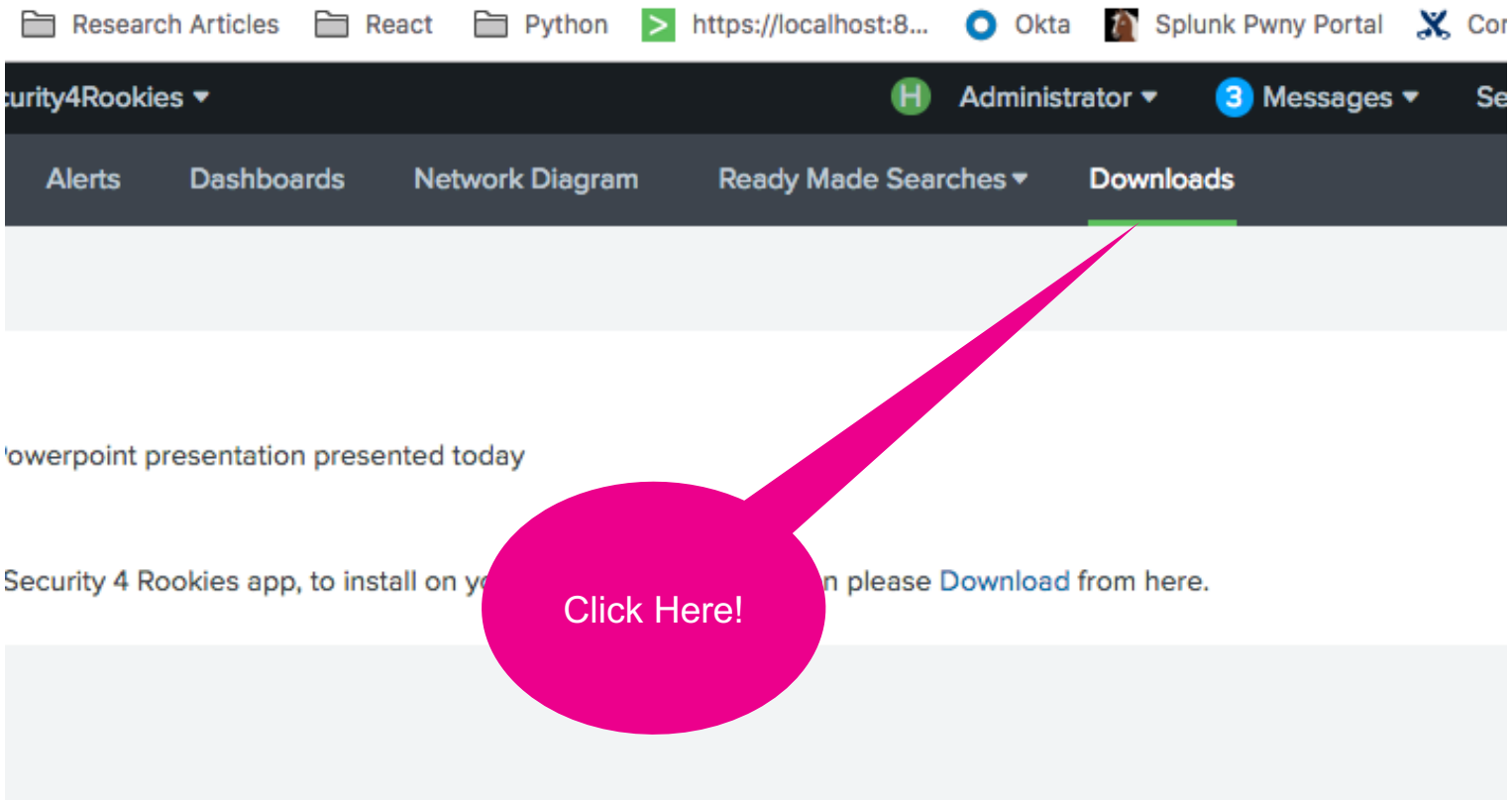
Security Dataset Project



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

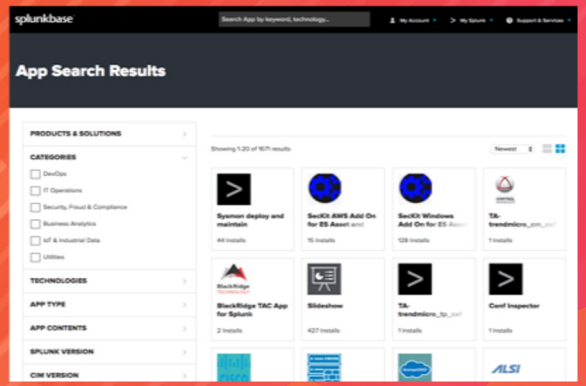
Todays Content

Download and play

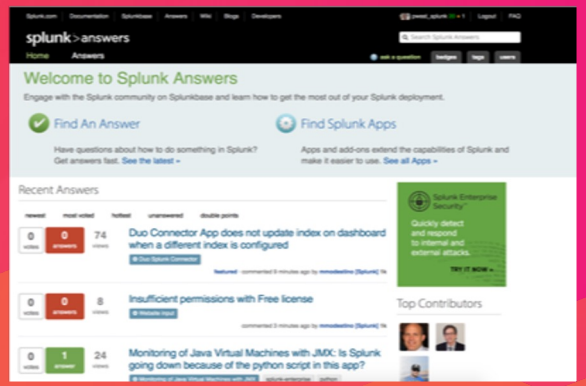


Thriving Community

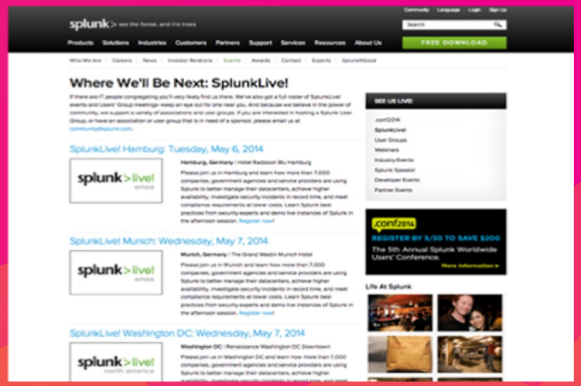
Splunkbase



Splunk Answers

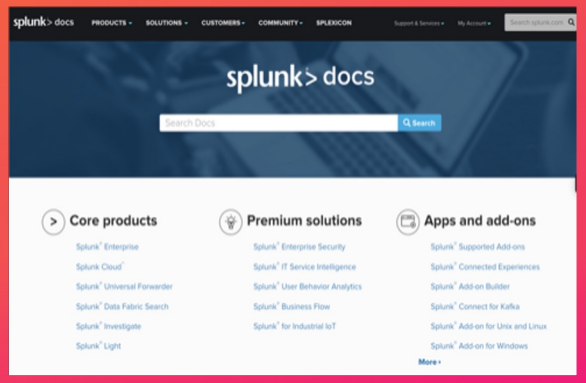


Splunk Events



Developer Resources

Documentation

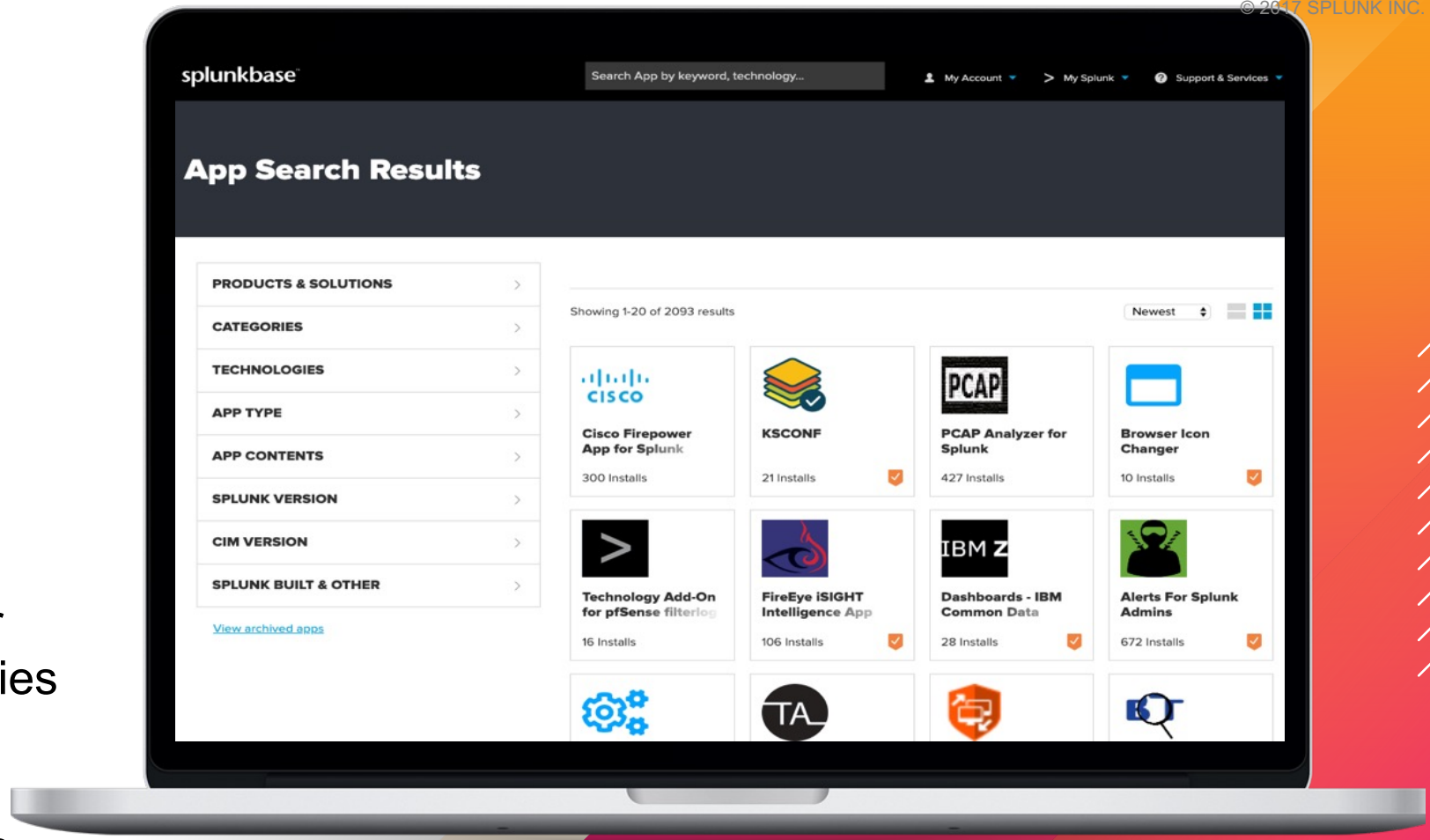


Education

Splunk Apps & Add-ons

https://splunkbase.com

- 2000+ 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!

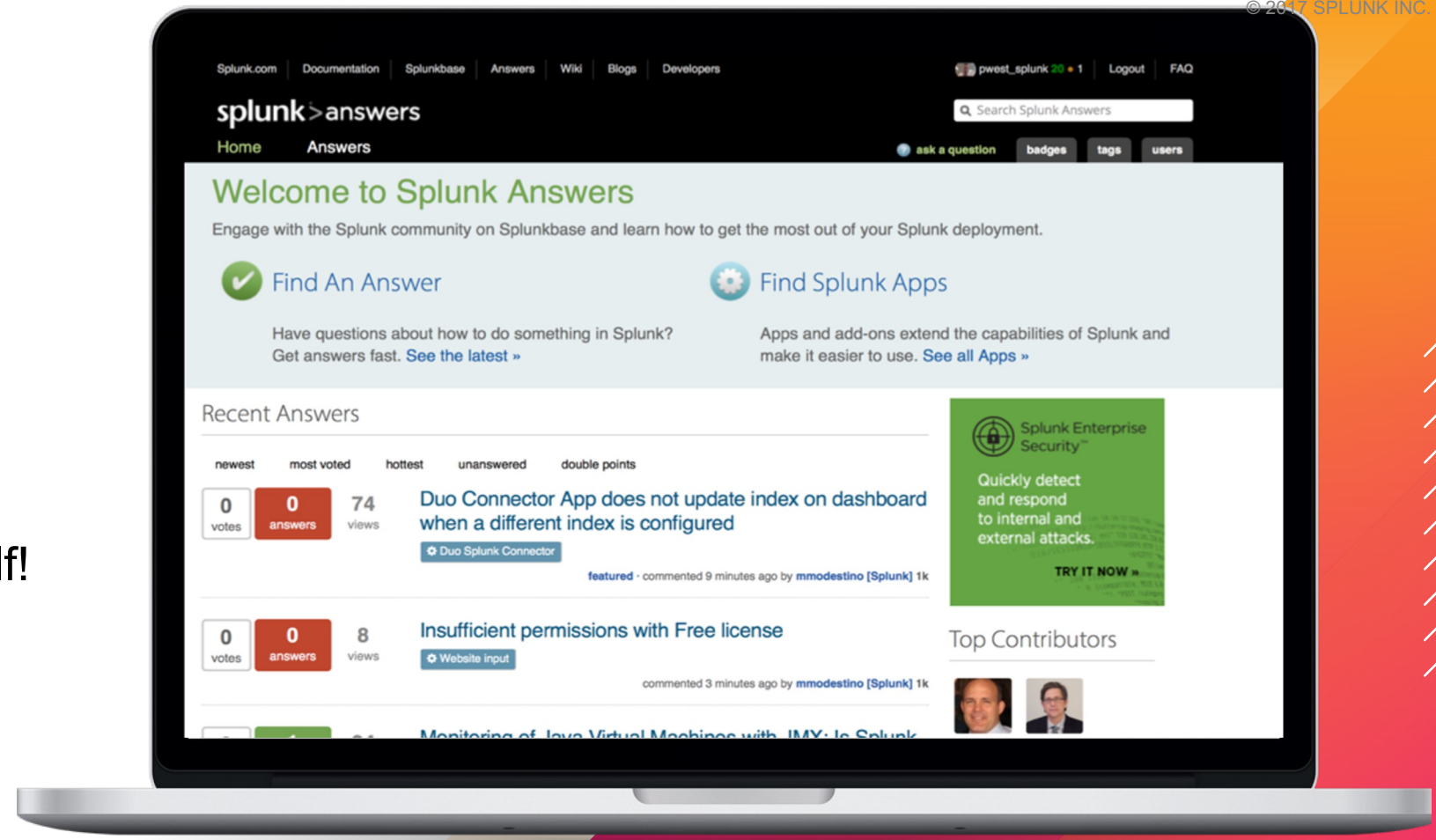


splunk> turn data into doing

Splunk Answers

https://answers.splunk.com

- Get answers to your questions from Splunk ‘know-it-all’s, or share what you've learned to achieve know-it-all status yourself!
- Engage with the Splunk community and learn how to get the most out of your Splunk deployment.

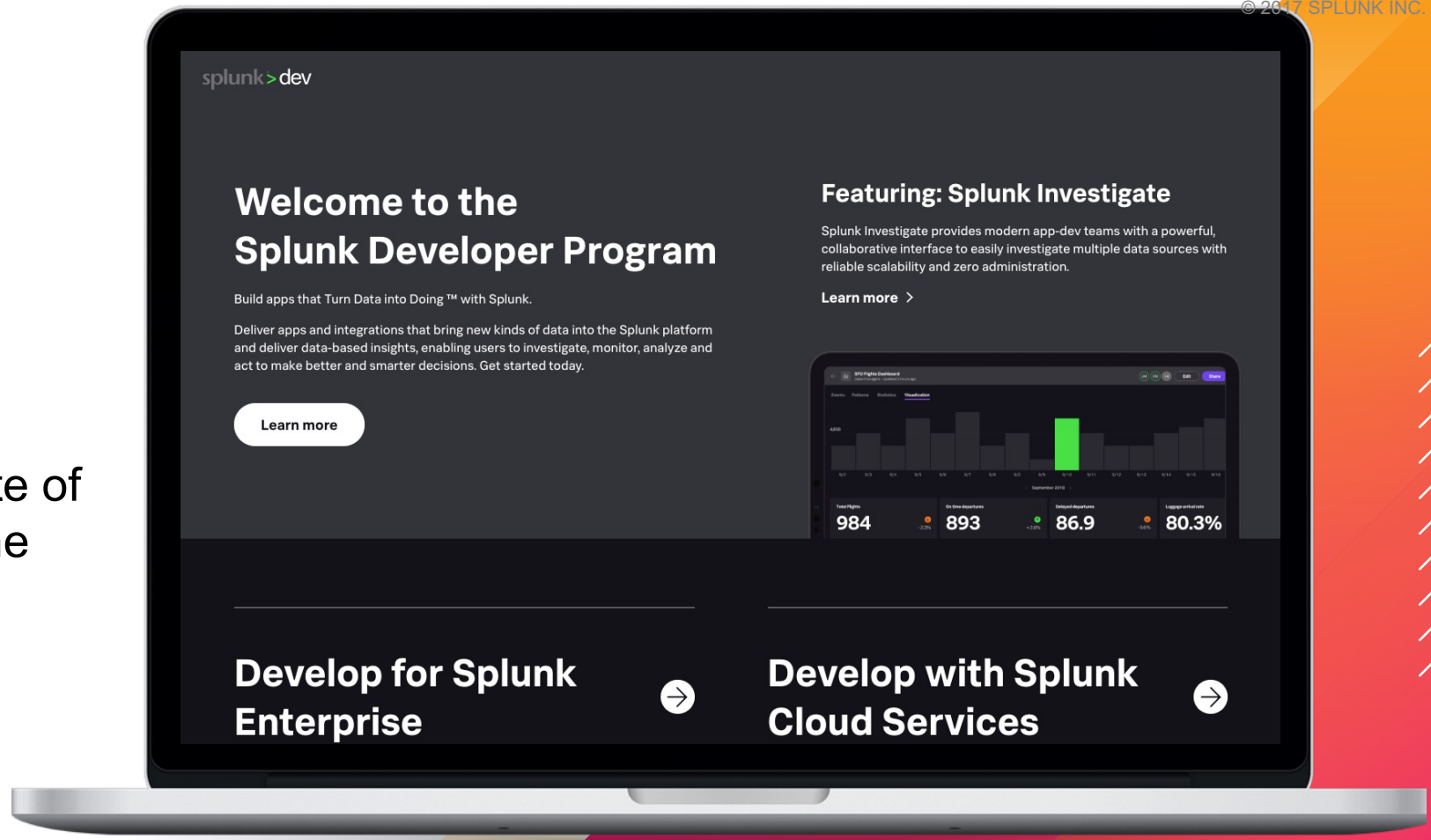


splunk> turn data into doing

Developer Resources

http://dev.splunk.com

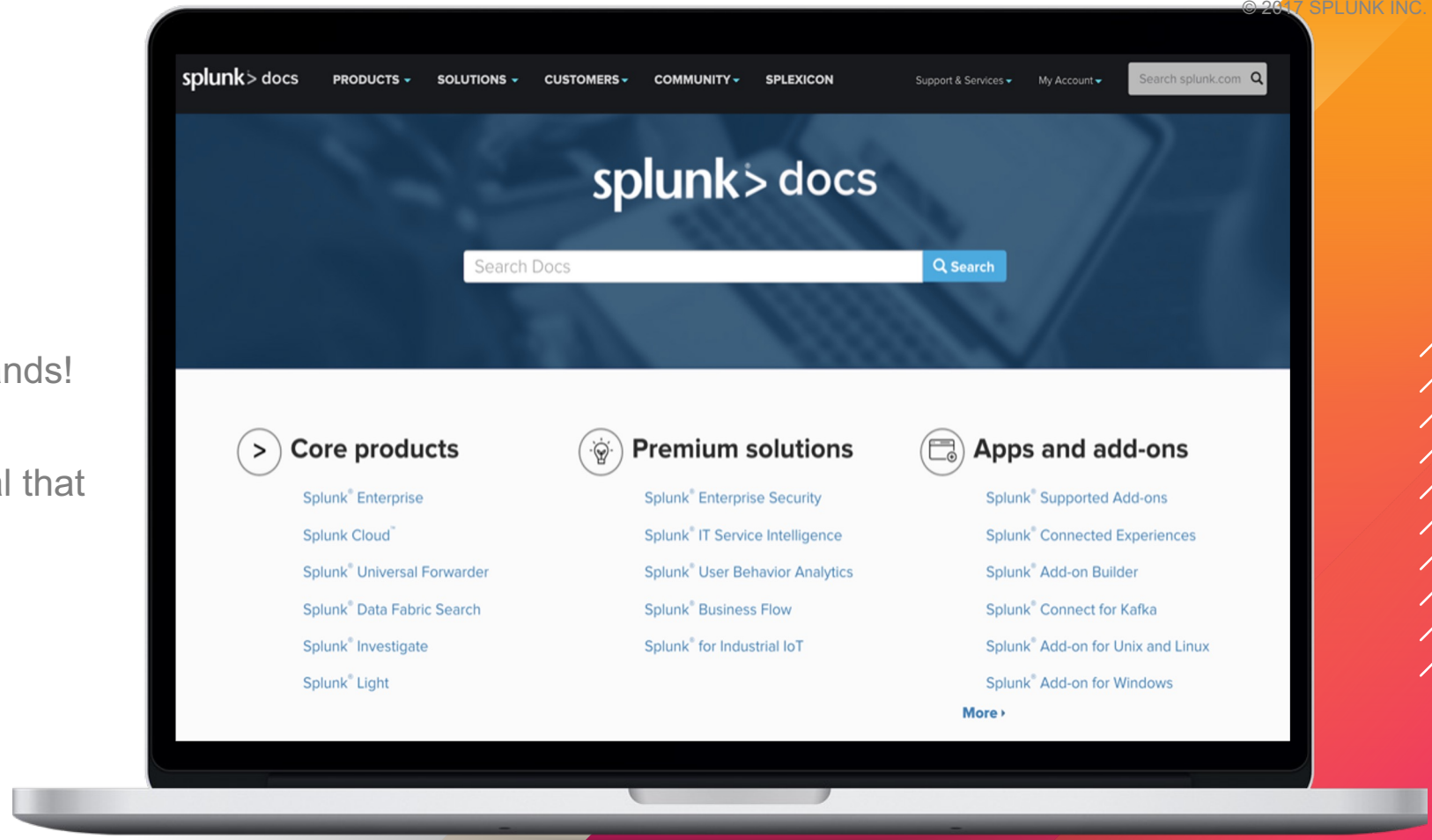
- Check out our REST API and suite of SDKs to customise and extend the power of Splunk
- Splunk integration with other applications and systems
- Resources for building Splunk apps
- Splunk Investigate



Documentation

https://docs.splunk.com

- Splunk reference – Learn the commands!
- Tutorials – Check out the search tutorial that even includes sample data to play with!
- Use cases
- References
- Procedures/guides – installing, upgrading
- And more!

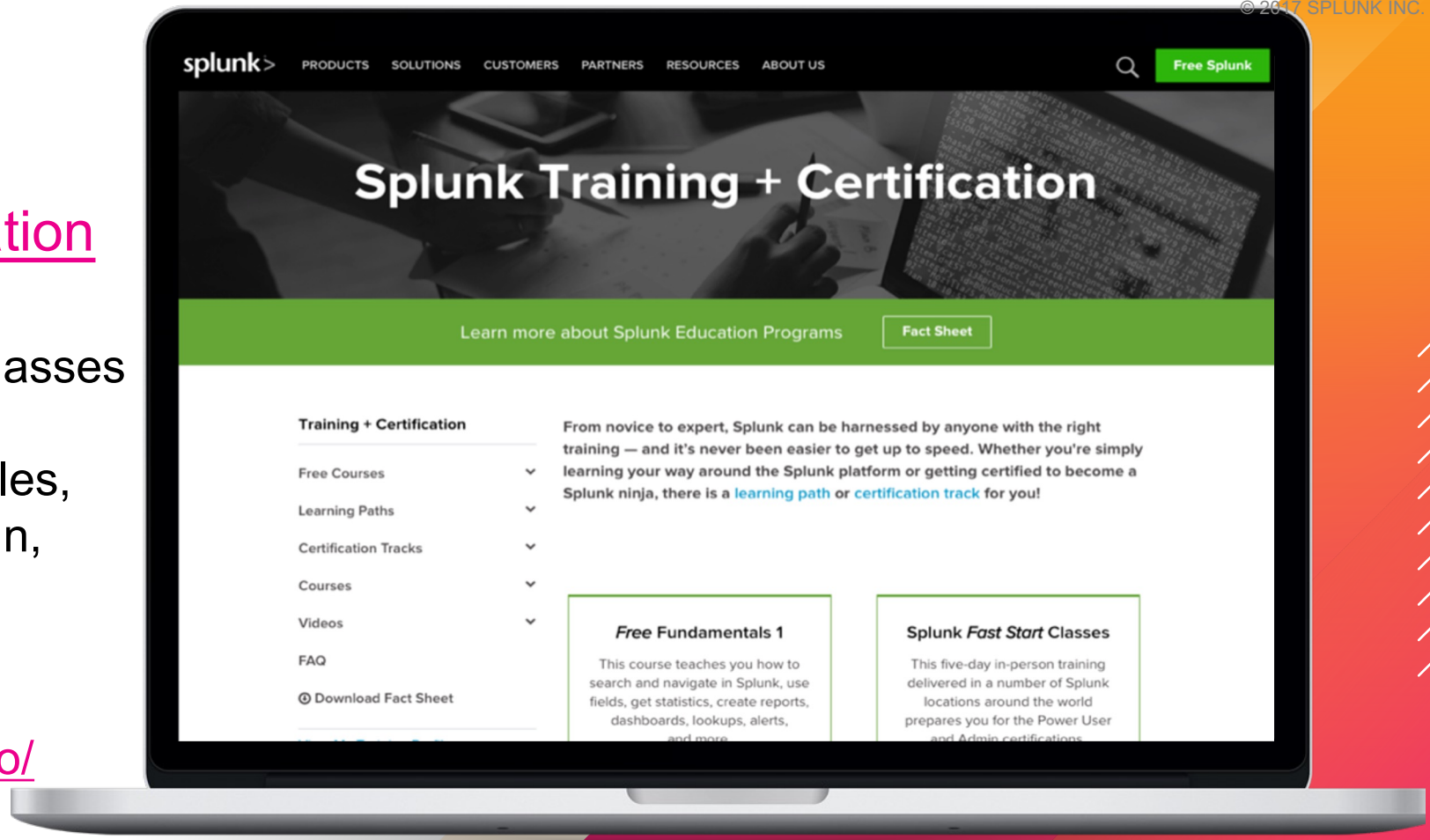


splunk> turn data into doing

Education

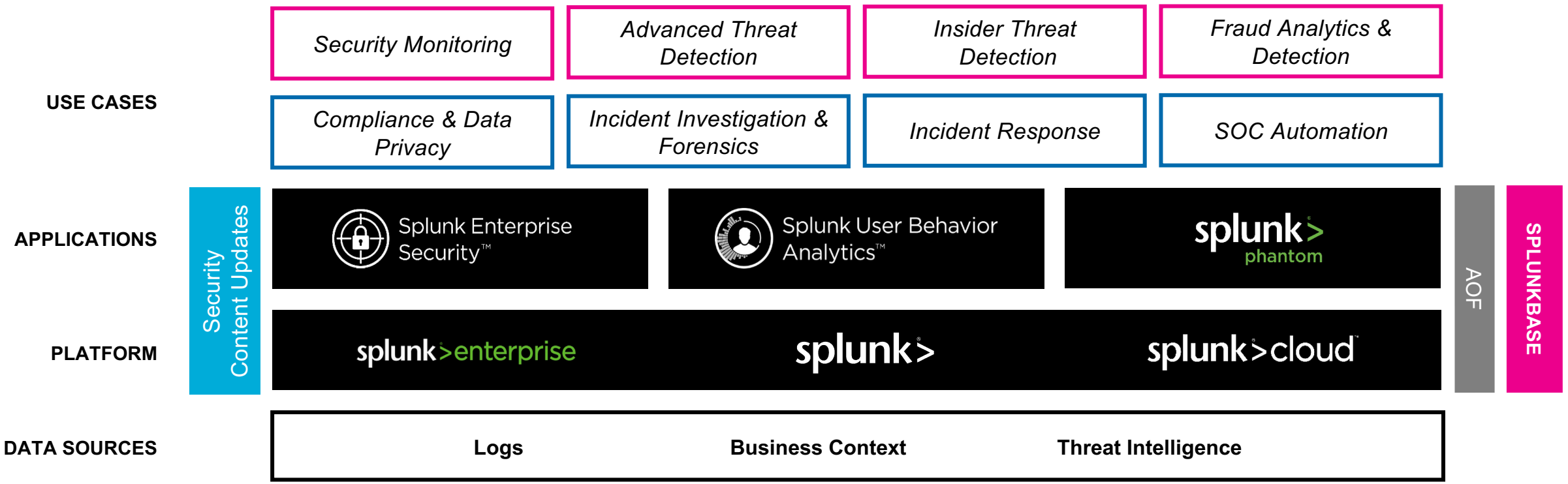
https://www.splunk.com/education

- Check out our online education classes
- Certification tracks for different roles, including User, Power User, Admin, Architect and Developer!
- Course examples: https://www.splunk.training/edemo/
- Free education!
  FREE: Online Splunk Fundamentals 1 course

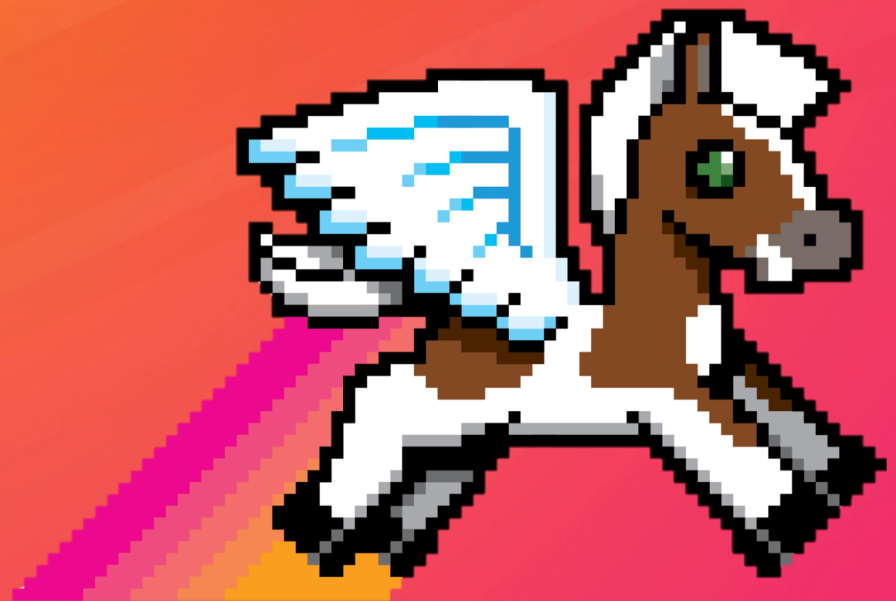


splunk> turn data into doing

Security Operations Suite



Thank You



splunk> turn data into doing™