

1. Register the lab environment:

[https://splunk4rookies.com/10411/self\\_register](https://splunk4rookies.com/10411/self_register)



# Splunk Security 4 Rookies

Daniel Yeung, Partner Technical Manager | Splunk

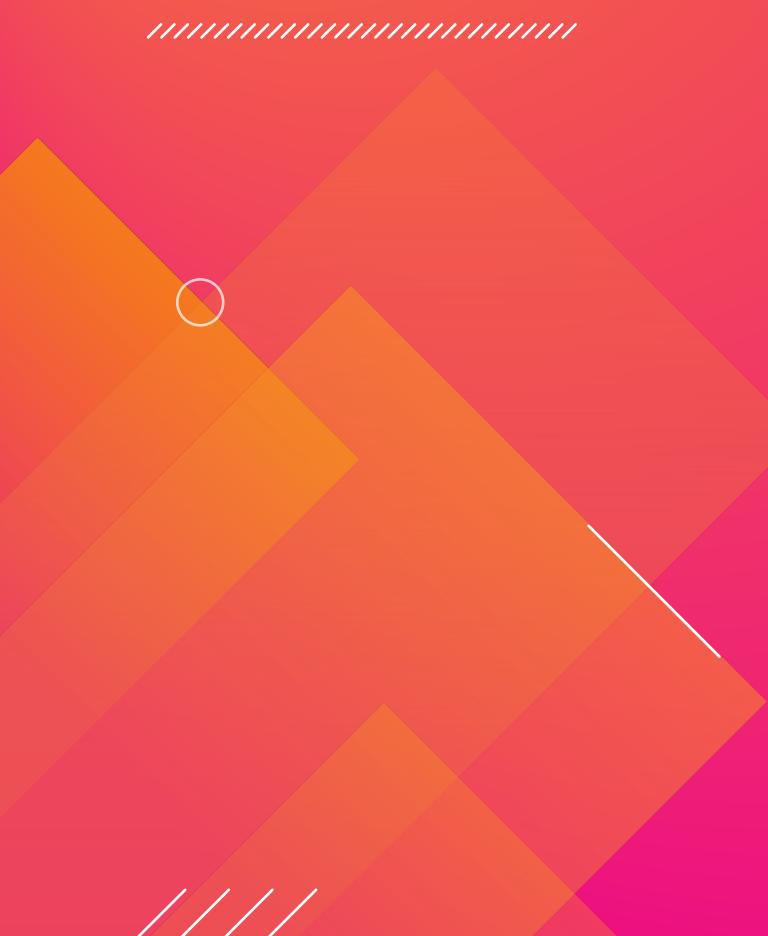


2. Download the presentation deck:

[https://drive.google.com/drive/folders/1wLkH44jjVWhKfy5F8yUhSJ78H7Z2FVb4?usp=share\\_link](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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

# Agenda for Today's Workshop



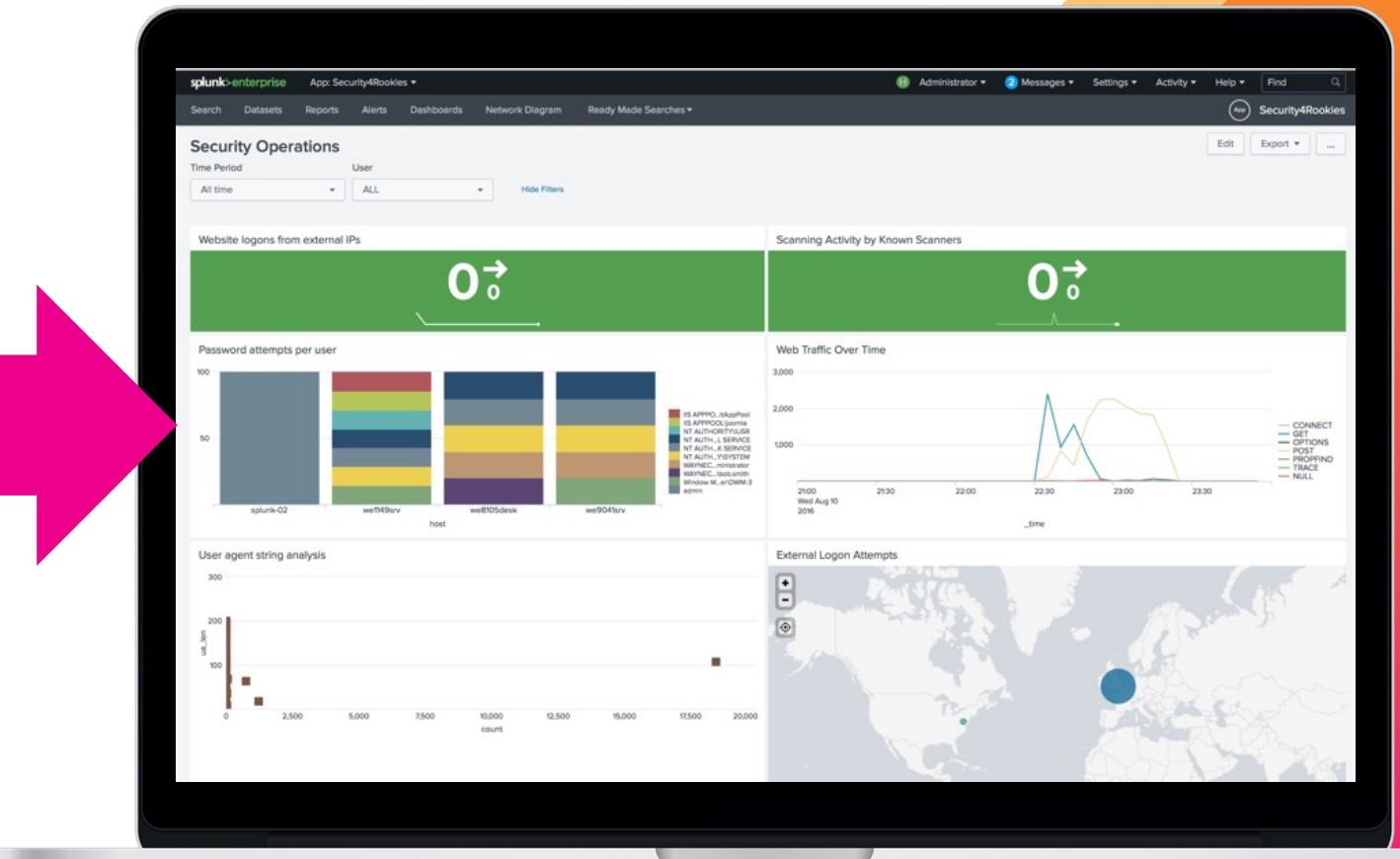
- ✓ Brief Splunk overview
- ✓ Search basics
- ✓ Indexing data
- ✓ Defining the format of your data
- ✓ Making data useable
- ✓ Aggregating and correlating data
- ✓ Put it into practice on web defacement investigation
- ✓ Creating proactive searches and dashboards

# 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" "Mozilla/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 3358 "http://www.myflowershop.com/category.screen?category_id=SURPRISE" "Mozilla/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" 200 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=SD1SL1  
HTTP 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=K  
9-BD-01&JSESSIONID=SD3SL1FF9ADFF7 HTTP 1.1" 404 664 "http://www.myflowershop.com/product.screen?product_id=K9-BD-01  
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=SD1SL7FF1ADFF10  
HTTP 1.1" 200 3770 "http://www.myflowershop.com/category.screen?category_id=BOUQUETS" "Mozilla/5.0 (Windows  
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=SD08SL3FF6ADFF10 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=SD02SL2FF7ADFF2  
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=SD08SL4FF9ADFF2  
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](https://splunk4rookies.com/10411/self_register)

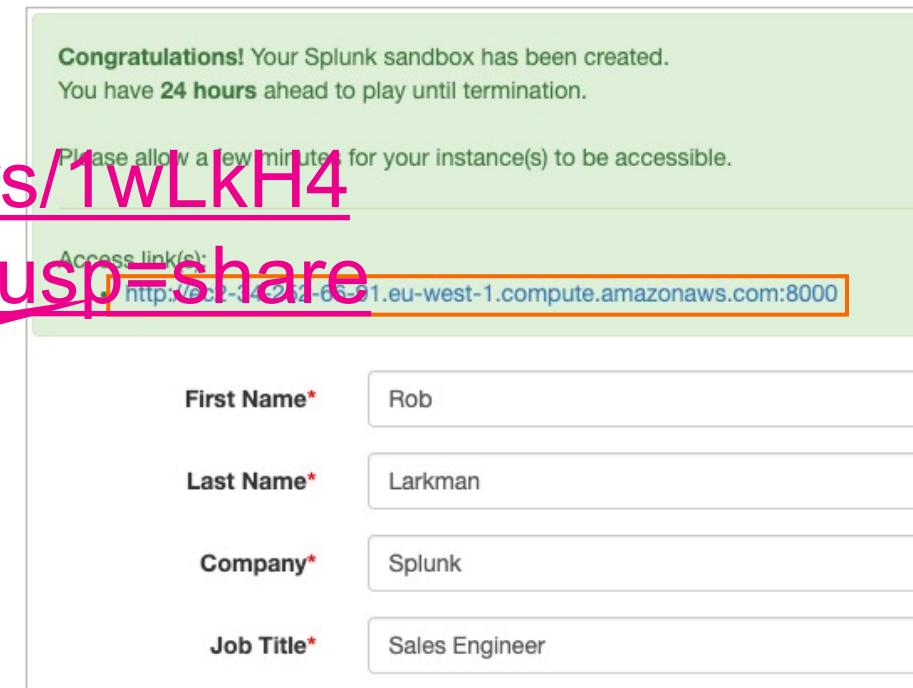


2. Download today's slide deck:

[https://drive.google.com/drive/folders/1wLKH44jjVWhKfy5F8yUhSJ78H7Z2FVb4?usp=share  
link](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!



Congratulations! Your Splunk sandbox has been created.  
You have **24 hours** ahead to play until termination.

Please allow a few minutes for your instance(s) to be accessible.

Access link(s):  
<http://ec2-34-231-65-51.eu-west-1.compute.amazonaws.com:8000>

First Name*	Rob
Last Name*	Larkman
Company*	Splunk
Job Title*	Sales Engineer

# Our World Never Stops Evolving.

New Ideas. New Devices. New Processes.

# 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

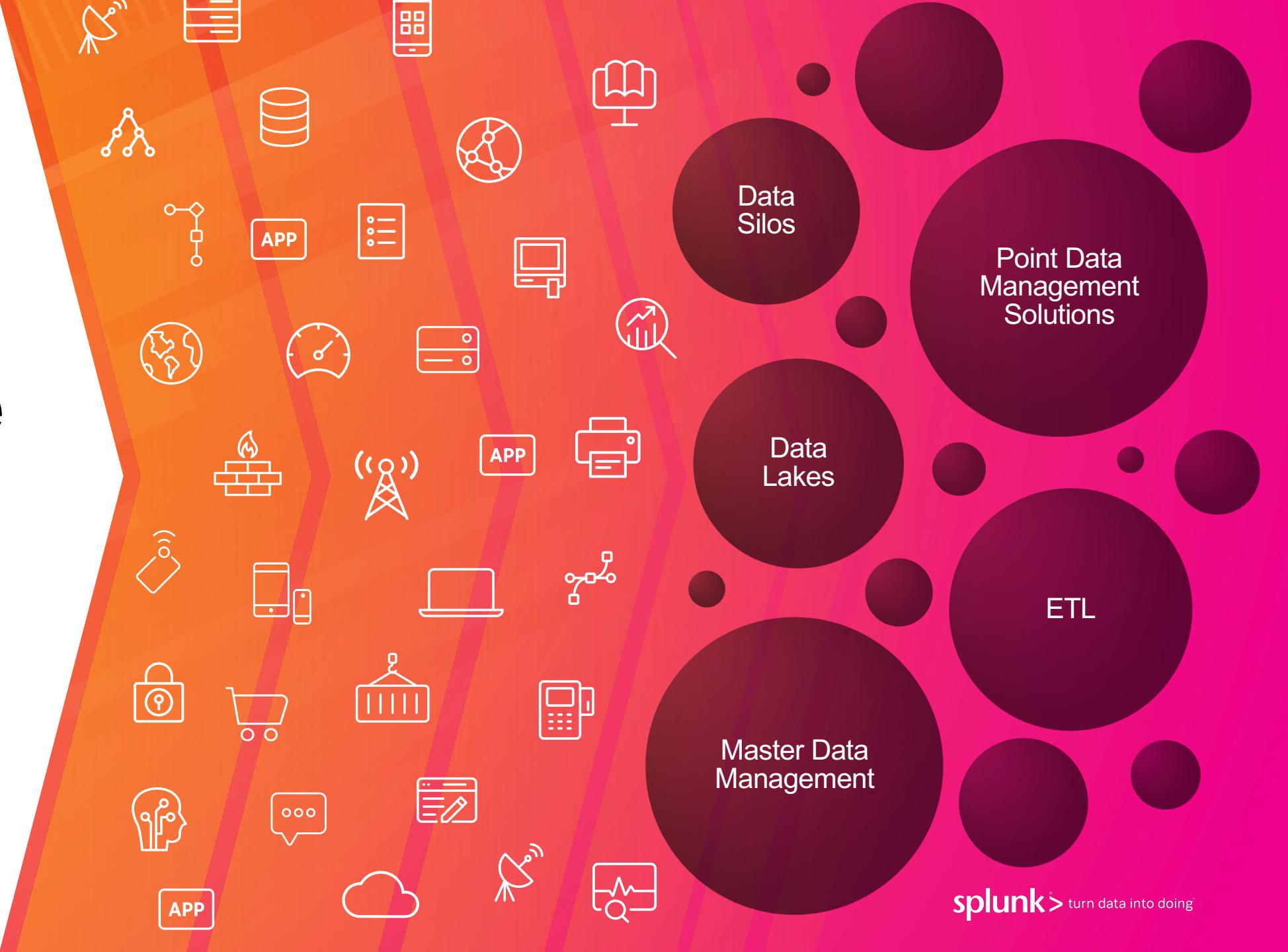
New  
Technology

New Data  
Streams

Networks

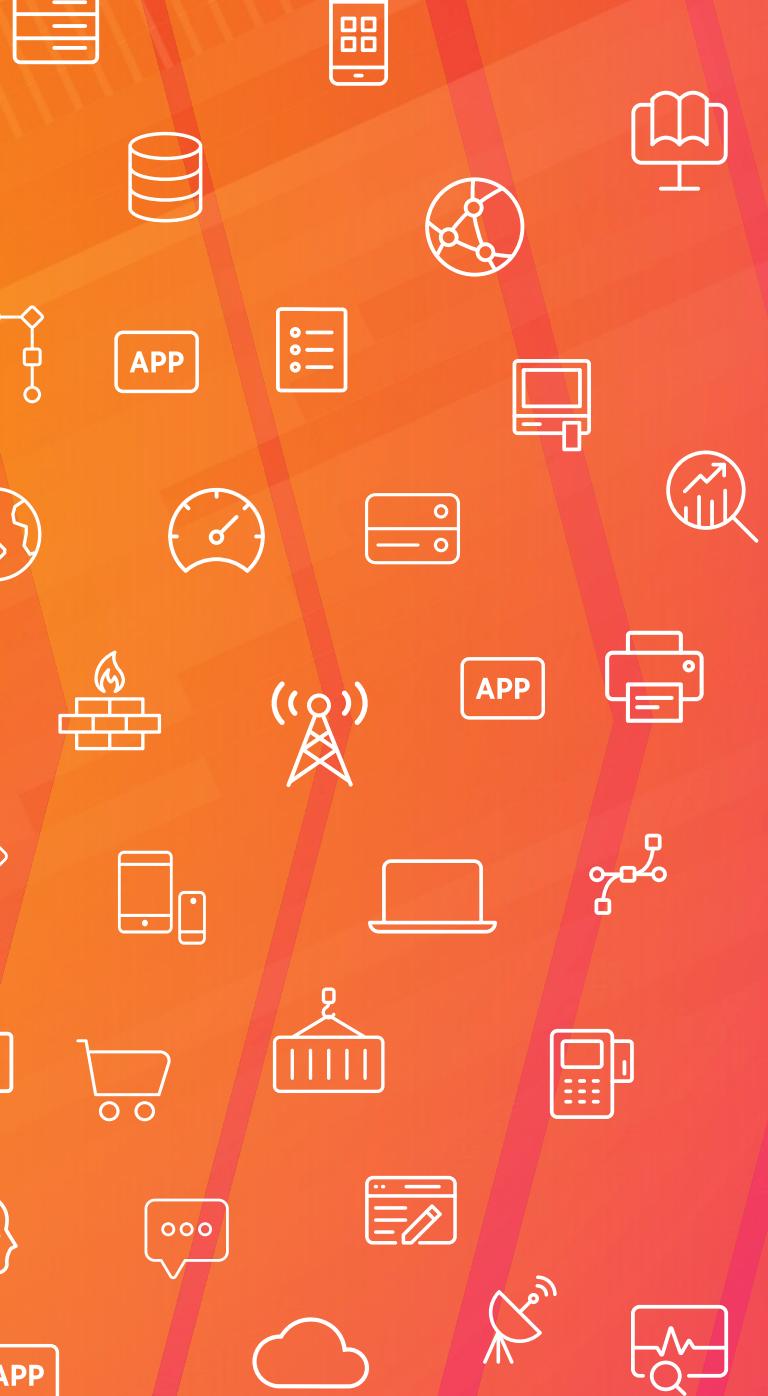
New  
Devices

# Turning Real-time Data Into Action is Hard



splunk®

# The Data-to-Everything Platform

**IT****Security****AppDev****Biz  
Analytics**

**Any Structure**  
**Any Source**  
**Any Time Scale**

**IT****Security****AppDev****Biz  
Analytics**

# Our Investigative Approach

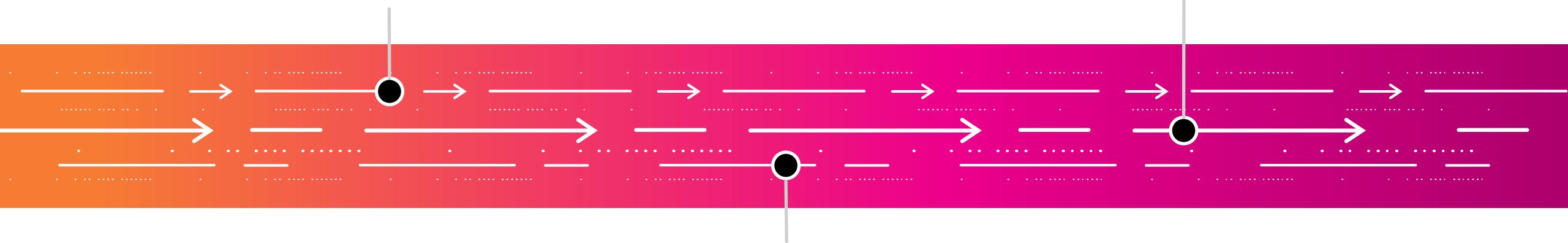
Adaptable | Real-Time | Fast To Value | Massive Scale

## Send

unstructured data from all  
systems, devices, and people

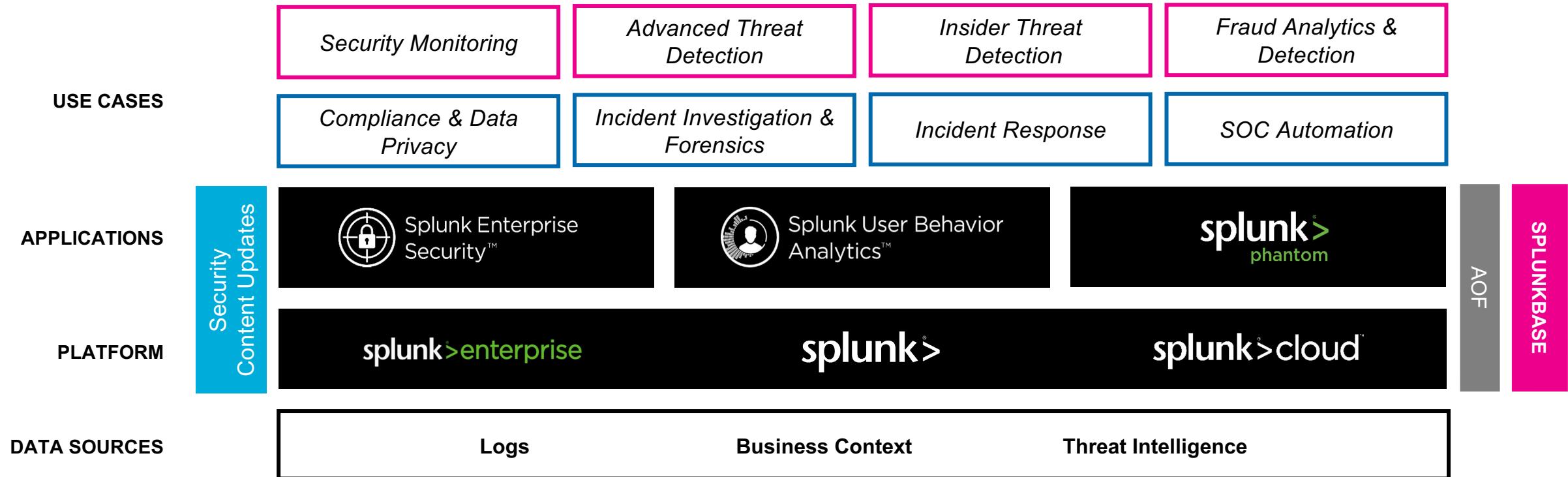
## React

quickly to changing circumstances by  
asking questions immediately

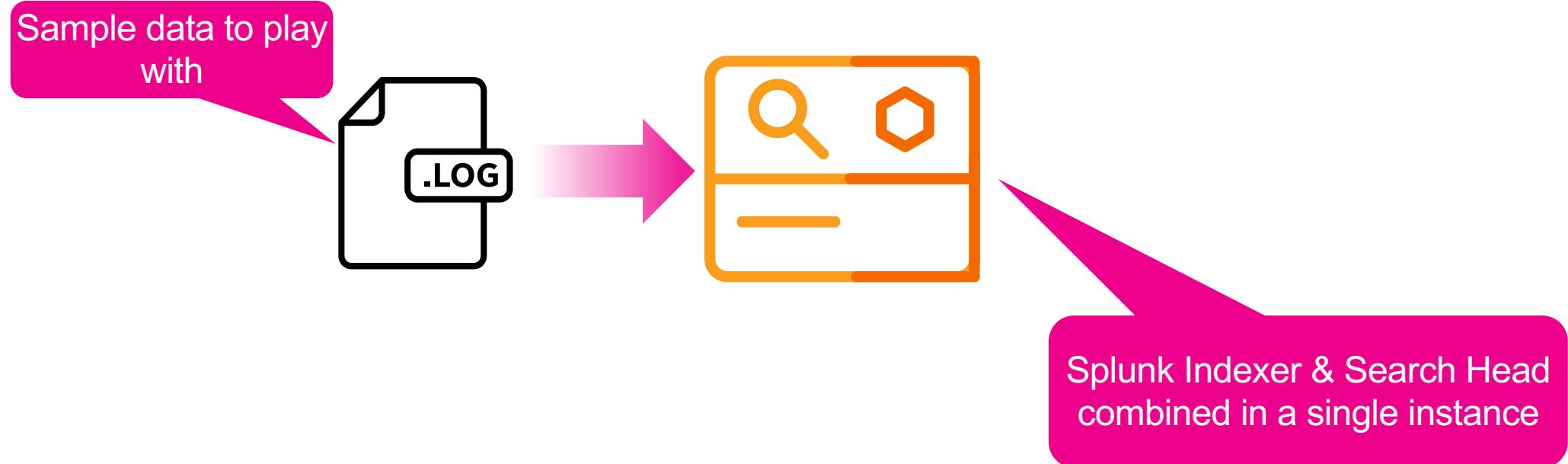


**Don't Structure**  
your data until you are ready

# Security Operations Suite

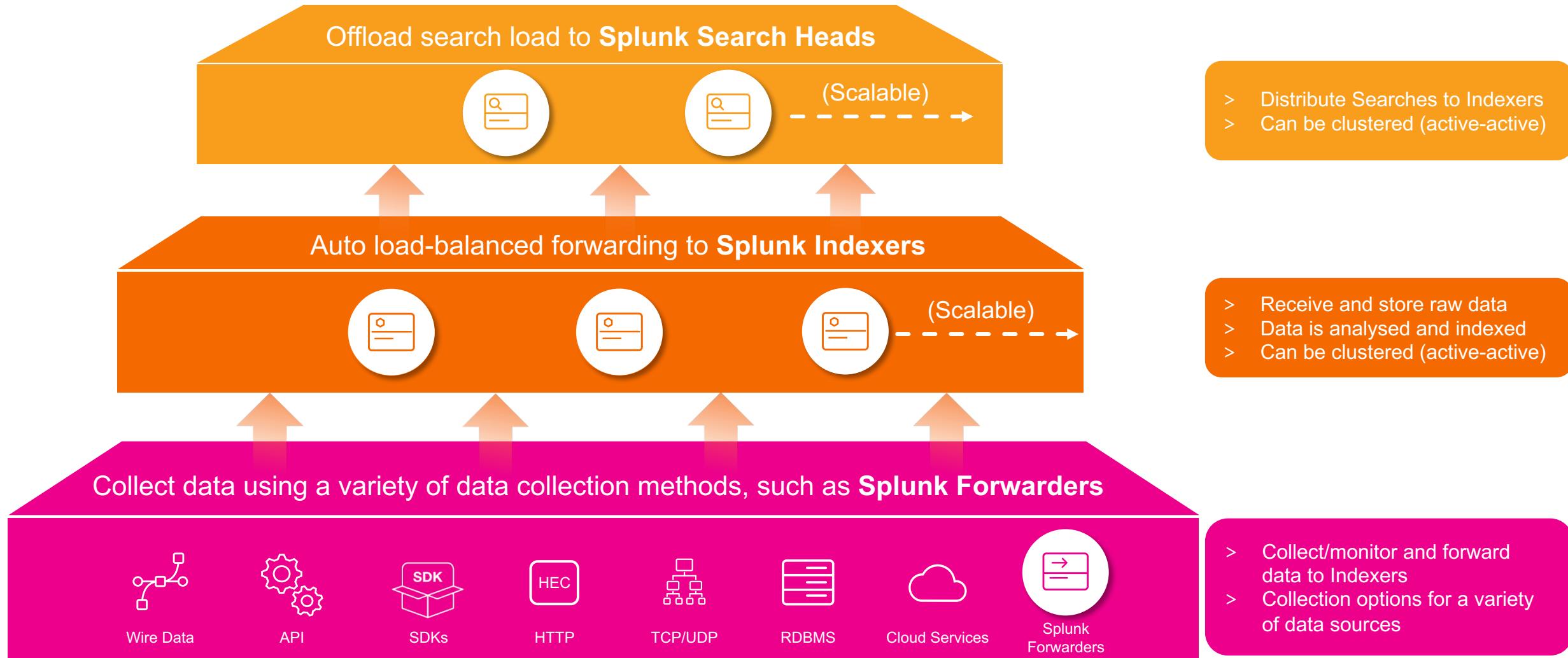


# Today's Environment



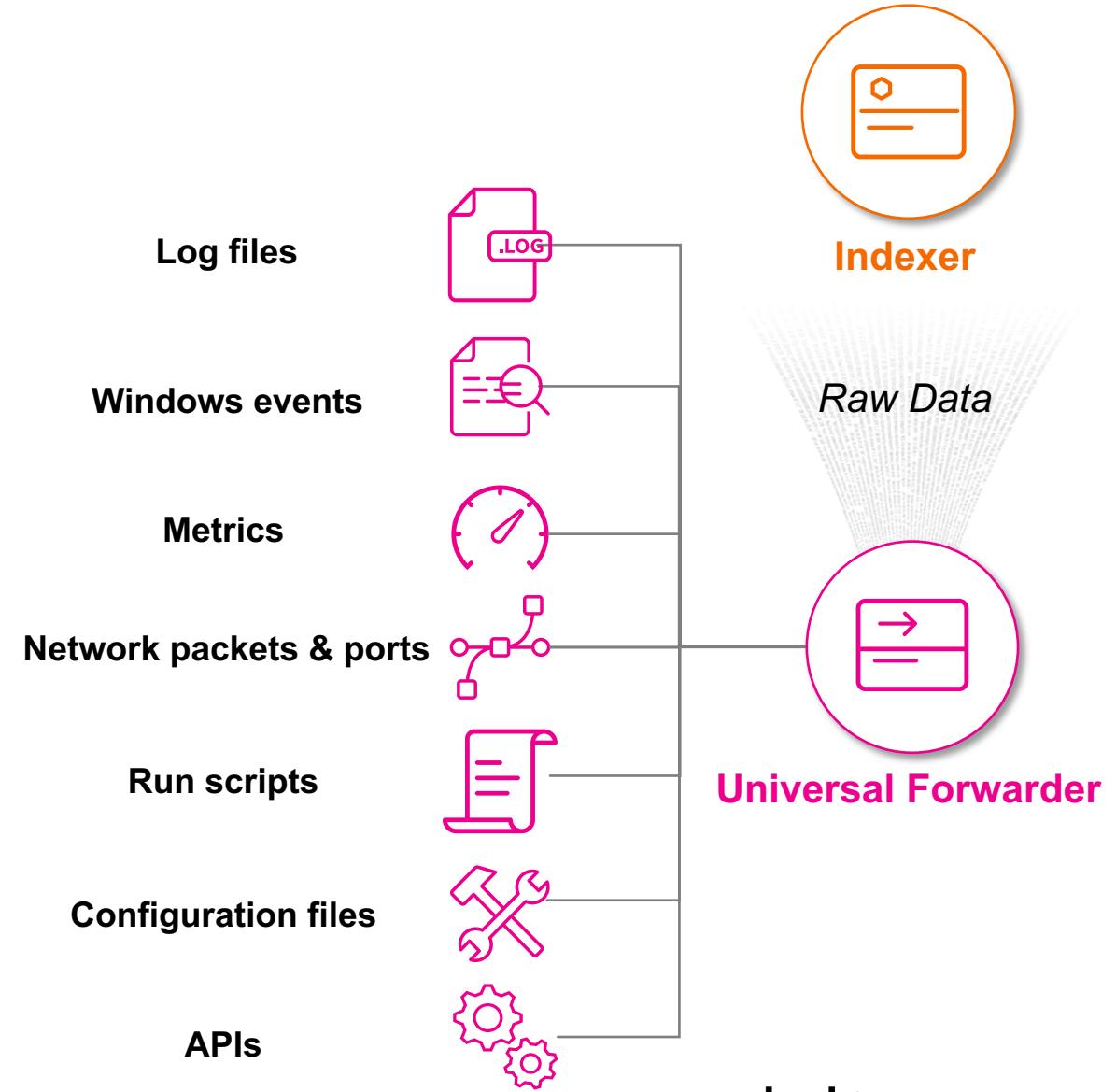
# Scales to Petabytes Per Day

Enterprise-Class Scale, Resilience and Interoperability



# 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](http://imreallynotbatman.com)

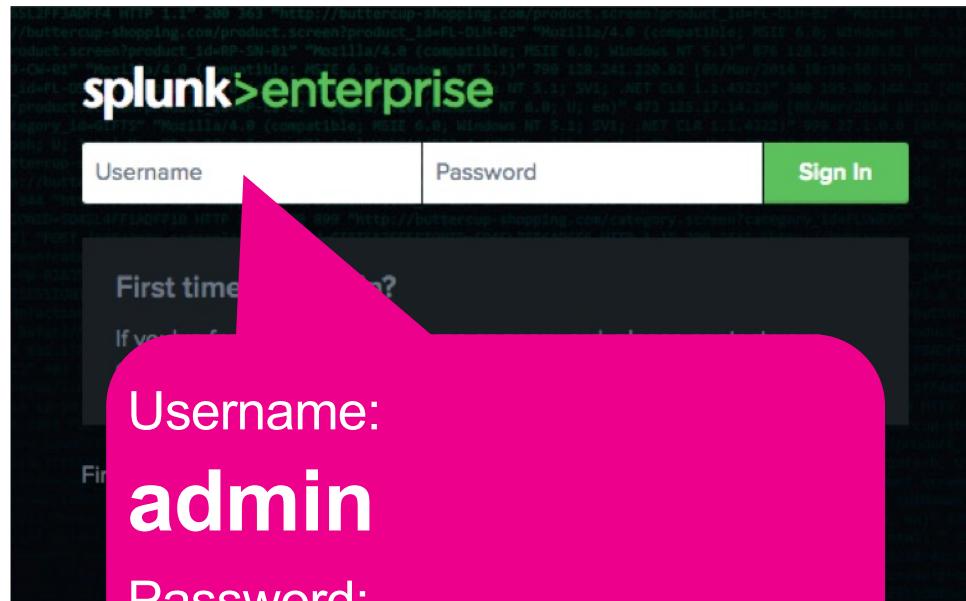
# Security Data and Searches

## For Security People



# Let's Go!

# Log in to Splunk



Default generic “app” for searching your data

Explore 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!



The screenshot shows the Splunk web interface with a dark theme. At the top, there's a navigation bar with tabs: Reports, Alerts, Dashboards, Network Diagram, Ready Made Searches (which has a pink '1' badge), and a dropdown arrow. A large, semi-transparent callout box is overlaid on the 'Ready Made Searches' tab. The callout box contains the following items:

- Chapter 1 - Search Basics **2** (highlighted with a blue border)
- Chapter 2 - Field Extraction
- Chapter 3 - EventTypes and
- Chapter 4 - Discovery
- Chapter 5 - Post Exploit

Below the callout box, there's a link: "Want to learn more about the search features, or want to learn more, see one of the following resources". To the right of the callout box, there's a vertical list of search results with small search icons next to them. A large pink arrow points from the bottom right towards the 'Click Here!' button. A pink oval surrounds the 'Click Here!' button.

App: Security4Rookies ▾

Reports    Alerts    Dashboards    Network Diagram    Ready Made Searches **1**

Chapter 1 - Search Basics **2**

Chapter 2 - Field Extraction

Chapter 3 - EventTypes and

Chapter 4 - Discovery

Chapter 5 - Post Exploit

Want to learn more about the search features, or want to learn more, see one of the following resources

Chpt1 - Search 1

Chpt1 - Search 2

Chpt1 - Search 3

Chpt1 - Search 4

Chpt1 - Search 5

at

955.8

INDEXED

Click Here!

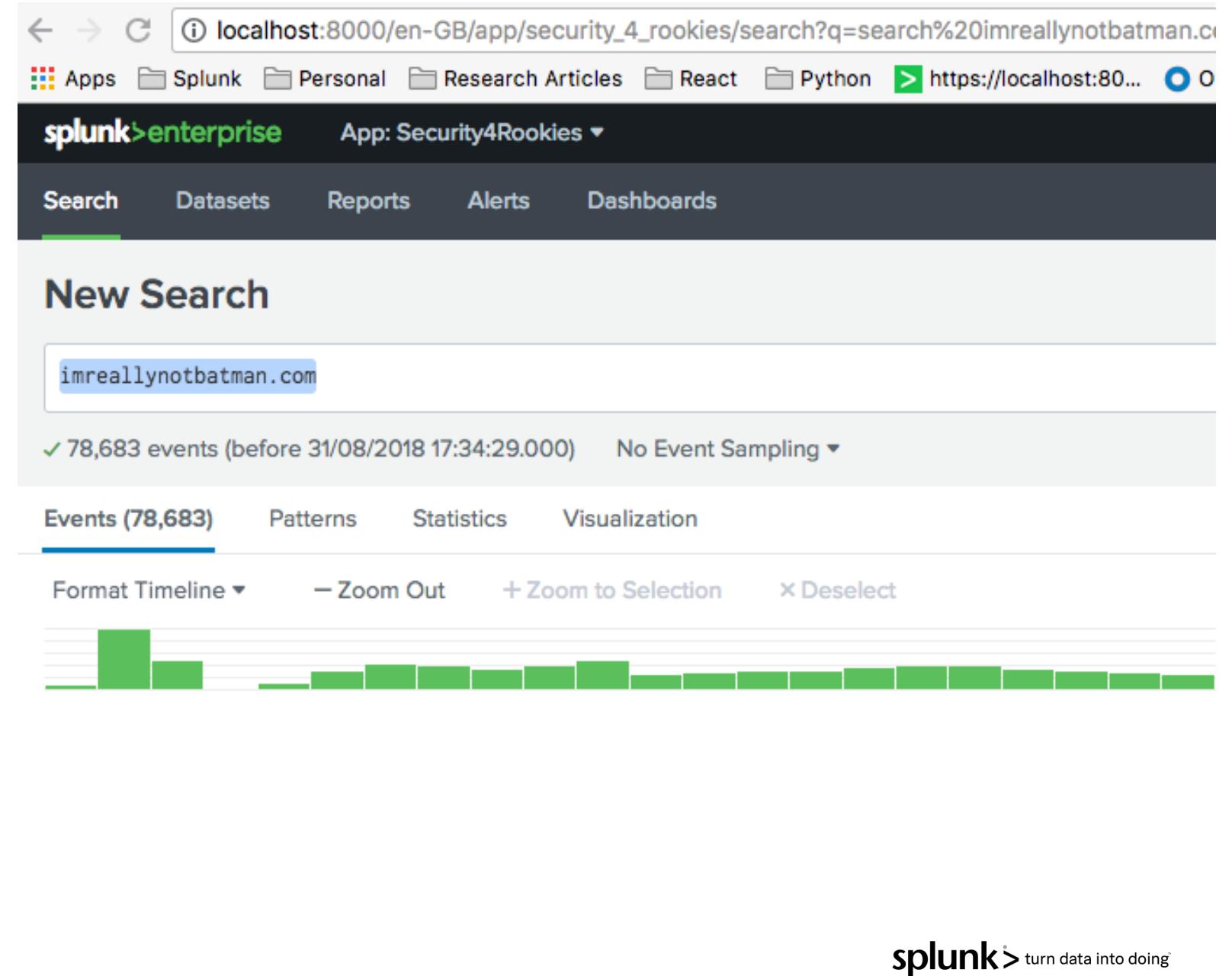
# Search Basics

## Chpt1 – Search 1

### Literal Strings

#### Manual

imreallynotbatman.com



# Search Basics

## Chpt1 – Search 2

Key=Value pair searching

### Manual

hostname="imreallynotbatman.com"

The screenshot shows the Splunk Enterprise search interface at [localhost:8000/en-GB/app/security\\_4\\_rookies/search?q=search%20hostname%3Dimreal](https://localhost:8000/en-GB/app/security_4_rookies/search?q=search%20hostname%3Dimreal). The search bar contains the query `hostname=imreallynotbatman.com`. Below the search bar, it says `13,915 events before 31/08/2018 17:38:03.000` and `No Event Sampling`. The interface includes tabs for `Events (13,915)`, `Fields`, `Statistics`, and `Visualization`. A pink callout bubble points from the search bar to a list of other search operators:

- Other Options**
- = equals
- != not equal to
- > greater than
- < less than
- >= greater or equal
- <= less than or equal to

**splunk> turn data into doing**

# Search Basics

## Chpt1 – Search 3

Using OR

### Manual

hostname="imreallynotbatman.com"

OR

hostname="www.microsoft.com"

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `hostname="imreallynotbatman.com" OR hostname="www.microsoft.com"`. Below the search bar, it says `✓ 13,919 events (before 31/08/2018 18:06:33.000)`. A pink callout bubble points from the word "OR" in the search bar to the following text:  
Remember Case Sensitivity  
`hostname="microsoft.com"`  
**NOT** the same as  
`HOSTNAME="microsoft.com"`

At the bottom right, the Splunk logo is visible: **splunk>** turn data into doing

# Search Basics

## Chpt1 – Search 4

Using Wildcards

Manual

\*3791

The screenshot shows the Splunk Enterprise search interface. The URL in the browser bar is `localhost:8000/en-GB/app/security_4_rookies/search?s=%2FservicesNS%2Fnobody%2F`. The top navigation bar includes links for Apps, Splunk, Personal, Research Articles, React, Python, and a link to `https://localhost:80...`. The main header displays "splunk>enterprise" and "App: Security4Rookies". Below the header, there are tabs for Search, Datasets, Reports, Alerts, Dashboards, and Ready Made Searches, with "Search" being the active tab. The main content area is titled "Chpt1 - Search 4". A search bar contains the query "\*3791". Below the search bar, it says "35 of 304,517 events matched" and "No Event Sampling". There are four tabs below the search bar: Events (35), Patterns, Statistics, and Visualization, with "Events (35)" being the active tab. Below these tabs are buttons for "Format Timeline", "Zoom Out", "Zoom to Selection", and "Deselect". A blue horizontal bar at the bottom right indicates the time "24 Aug 2016 17:5".

# Search Basics

## Chpt1 – Search 5

### Using Wildcards

#### Manual

3791\*exe

The screenshot shows the Splunk Enterprise search interface at [localhost:8000/en-GB/app/security\\_4\\_rookies/search?q=search%203791\\*exe&display.page](https://localhost:8000/en-GB/app/security_4_rookies/search?q=search%203791*exe&display.page). The search bar contains "3791\*exe". Below it, a message indicates "11 events (before 31/08/2018 18:44:01.000) No Event Sampling". The "Events (11)" tab is selected. A timeline at the bottom shows three green bars representing event intervals. At the bottom right, there are buttons for "List", "Format", and "20 Per Page".

# 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

## New Search

192.168.250.0/24

✓ 65 events (before 15/10/2018 15:18:29.000) No Event Sampling ▾

Events (65)

Patterns

Statistics

Visualization

Format Timeline ▾

– Zoom Out

+ Zoom to Selection

✗ Deselect

Raw ▾

✓ Format

20 Per Page ▾

< Hide Fields

☰ All Fields

#### SELECTED FIELDS

↳ host 1  
↳ source 4  
↳ sourcetype 1

#### INTERESTING FIELDS

↳ control 1  
# count 9  
↳ edit\_allowed 1  
# folder\_id 1

i

Event

```
↳ { [-]
    control: true
    count: 20
    edit_allowed: true
    folder_id: 2
    hasaudittrail: true
    haskb: true
    host-ip: 192.168.250.100
    host_id: 101
    host_start: Wed Aug 24 10:33:51 2016
```

**splunk** > turn data into doing

# Search Basics

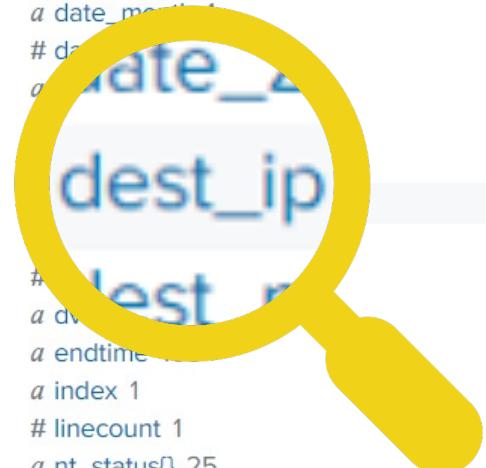
## Chpt1 – Search 6

### CIDR Matching

#### Manual

dest\_ip=192.168.250.0/24

```
# bytes_in 100+
# bytes_out 100+
# command[] 20
# date_hour 9
# date_mday 2
# date_minute 60
# date_month 1
# date_year 1
# dest_ip 7
# dest_port 1
# duration 1
# endtime 1
# index 1
# linecount 1
# nt_status[] 25
# packets_in 100+
# packets_out 100+
# punct 100+
```



**dest\_ip**

7 Values, 100% of events  Selected

**Reports**

[Top values](#) [Top values by time](#) [Rare values](#)

[Events with this field](#)

Values	Count	%
192.168.250.20	122,213	41.231%
192.168.250.100	80,228	27.067%
192.168.250.70	63,958	21.578%
192.168.250.40	17,782	5.999%
192.168.250.41	11,472	3.87%
192.168.250.255	702	0.237%
192.168.250.1	52	0.018%

L\_endtime : 2010-06-24T10:27:45.273003Z , timestamp : 2010-06-24T10:27:27.013472Z

# Splunk's 'Search Processing Language' (SPL)

Search terms

`dest_ip=192.168.250.70`

Commands

`| stats count by src_ip | rename count as requests`

Pipe character:  
Output of left is input to right

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'><System>5698FFBD9>/><EventID>3</EventID><Version>5</Version><Level>4</Level><TaskSystemTime>'2016-08-24T18:19:15.575237300Z'</EventRecordID>3705233</Event>crossoft-Windows-Sysmon/Operational</Channel><Computer>we9041srv.waynecorp<='UtcTime'>2016-08-24 18:20:05.127</Data><Data Name='ProcessGuid'>{46C7284='Image'>System</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='Ipv6'>false</Data><Data Name='SourceIp'>192.168.250.20</Data><Data Name='\$Data'><Data Name='SourcePortName'>microsoft-ds</Data><Data Name='Destinat<='DestinationHostName'></Data><Data Name='DestinationPort'>64108</Data><Data Name='host'>we9041srv</Data><source>WinEventLog:Microsoft-Windows-Sysmon/Operational</source>
>	24/08/2016 18:04:15.000	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>5698FFBD9>/><EventID>3</EventID><Version>5</Version><Level>4</Level><TaskSystemTime>'2016-08-24T18:04:15.604356700Z'</EventRecordID>3701741</Event>crossoft-Windows-Sysmon/Operational</Channel><Computer>we9041srv.waynecorp<='UtcTime'>2016-08-24 18:05:05.126</Data><Data Name='ProcessGuid'>{46C7284='Image'>System</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='Ipv6'>false</Data><Data Name='SourceIp'>192.168.250.20</Data><Data Name='\$Data'><Data Name='SourcePortName'>microsoft-ds</Data><Data Name='Destinat<='DestinationHostName'></Data><Data Name='DestinationPort'>6408</Data><Data Name='host'>we9041srv</Data><source>WinEventLog:Microsoft-Windows-Sysmon/Operational</source>

`| 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

Functions

`| 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>

# 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 audit
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-acl 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

The screenshot shows two instances of the Splunk Enterprise interface. Both instances have the search bar set to "index=botsv1 sourcetype=fgt\_utm".

**Left Instance (Step 1):** Shows a single event in the "Event" view. A pink arrow labeled "1" points to the "Event Actions" button. The event details are as follows:

```

24/08/2016 19:27:14.000
Aug 24 12:27:14 192.168.250.1 date=2016-08-24 time=12:27:14 devname=gotham-fortigate
vel=information vd="root" appid=16270 user="" srcip=192.168.250.41 srcport=51108
srcd=4237598 applist="Honeypot-Access" appcat="Network.Service" app="NTP" action=pass ms=100

```

**Right Instance (Step 2):** Shows the same event with the "Type" dropdown open, displaying "Selected". A pink arrow labeled "2" points to the "Selected" option.

**Bottom Instance (Step 3):** Shows the "Event Actions" menu open. A pink arrow labeled "3" points to the "Build Event Type" button. The menu options are:

- Build Event Type
- Extract Fields
- Show Source

The "Event" view below the menu lists fields and their values:

Field	Value
host	192.1
source	udp:1
sourcetype	fgt_
action	allow
app	NTP
appcat	Netw
appid	1627

# Field Extraction Basics

## Chpt2 – Search 1

Extract the field

The screenshot shows the 'Extract Fields' process in Splunk. The current step is 'Select Method'. The 'Source type' is set to 'fgt\_utm'. Below it, a log entry is displayed:

```
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 srcip=192.168.250.41 srcport=51108 srcintf="internal3" dstip=91.189.91.157 dstport=123 proto=17 service="NTP" policyid=10 sessionid=4237590 applist="Honeypot-Access" appcat="Network.Service" app="NTP" action=pass msg="Network.Service: NTP," apprisk=elevated
```

The 'Select Method' section contains two options:

- Regular Expression:** Contains the regular expression `(.*?)`. A pink arrow labeled '1' points to this section.
- Delimiters:** Contains the delimiter `x|y|z`.

A green 'Next >' button is located at the top right of the step header. A pink arrow labeled '2' points to this button.

# Field Extraction Basics

Chpt2 – Search 1

Highlight and Name

localhost:8000/en-GB/app/security\_4\_rockies/field\_extractor?sid=1535970647.17&offset=0

Apps Splunk Personal Research Articles React Python https://localhost:80... Okta Splunk Pwny Portal

splunk>enterprise App: Security4Rookies Extract Fields Select Method Select Fields Validate

### Select Fields

1. Highlight field

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in every event part of an existing extraction, first turn off the existing extractions. [Learn more](#)

Aug 24 12:27:14 192.168.250.1 date=2016-08-24 time=12:27:14 devname=gotham-fortigate devid=FGT60D4614044725 logid=1059 srcip=192.168.250.1 dstip=91.189.91.157 dstport=123 proto=17 service="NTP" policyid=1 msg=

Extract    Require

Field Name: src\_ip    2

Sample Value: 192.168.250.1

Add Extraction    3

1. Highlight field

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in every event part of an existing extraction, first turn off the existing extractions. [Learn more](#)

Aug 24 12:27:14 192.168.250.1 date=2016-08-24 time=12:27:14 devname=gotham-fortigate devid=FGT60D4614044725 logid=1059 srcip=192.168.250.1 dstip=91.189.91.157 dstport=123 proto=17 service="NTP" policyid=1 msg=

Extract    Require

Field Name: src\_ip    2

Sample Value: 192.168.250.1

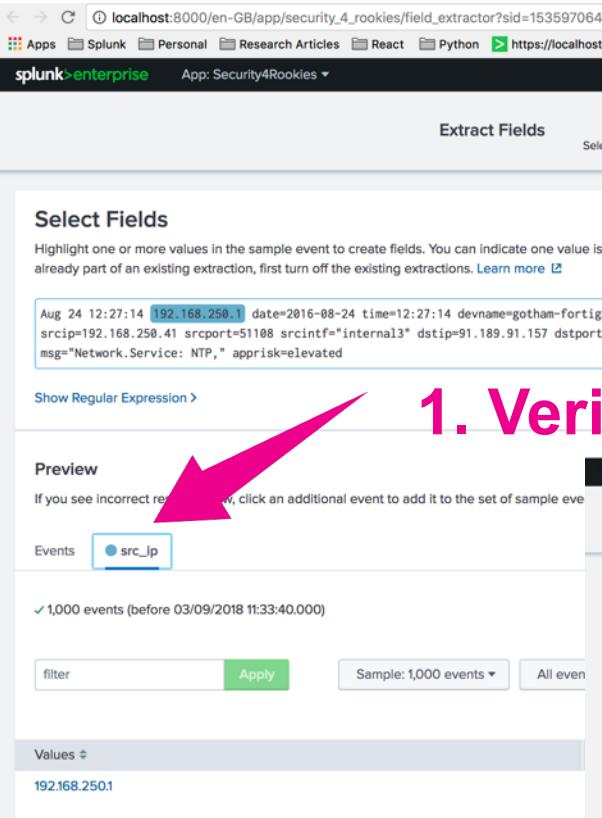
Add Extraction    3

# Field Extraction Basics

## Chpt2 – Search 1

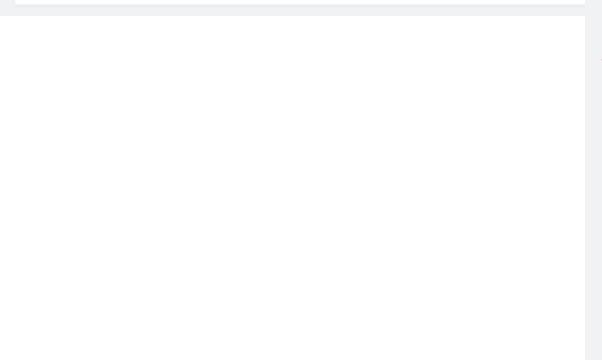
### Verify Fields and Set Access Rights

**1. Verify Values**



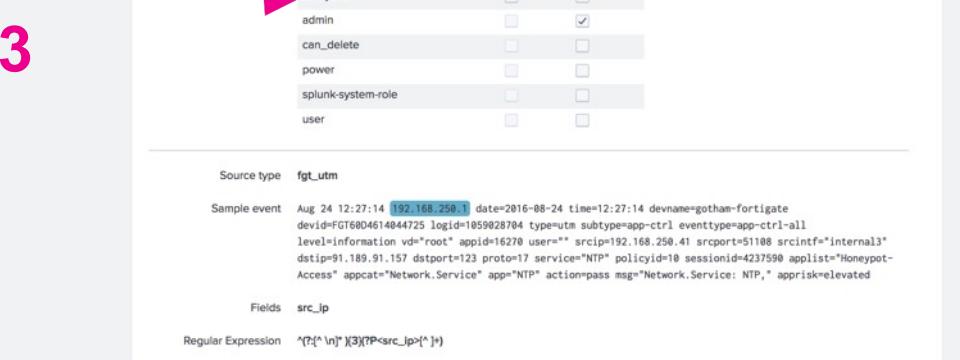
The screenshot shows the 'Extract Fields' wizard in Splunk. The current step is 'Select Fields'. The interface includes a preview of sample event data, a 'Show Regular Expression' button, and a 'Preview' section. In the 'Preview' section, a pink arrow points to the 'Values' dropdown, which contains the value '192.168.250.1'. The status bar at the bottom indicates '1,000 events (before 03/09/2018 11:33:40.000)'.

**2**



A pink arrow points to the green 'Next >' button at the top right of the 'Select Fields' step.

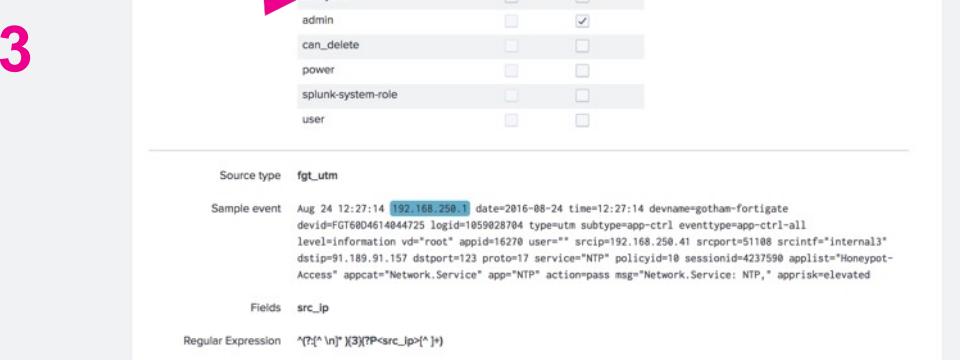
**3**



A pink arrow points to the 'App' tab in the 'Permissions' table under the 'Save' step. The table lists users and their permissions for the extraction named 'EXTRACT- src\_ip'.

User	Owner	App	All apps
everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**4**



A pink arrow points to the green 'Finish >' button at the top right of the 'Save' step.

# 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

Search for specific records

Windows Logon Success Event

Eventtype

win\_auth\_success

Tag

Linux Logon Success Event

} nix\_auth\_success

success

Tag

VPN Logon Success Event

} vpn\_auth\_success

authentication

Windows Logon Failure Event

} win\_auth\_failure

Linux Logon Failure Event

} linux\_auth\_failure

failure

VPN Logon Failure Event

} vpn\_auth\_failure

# Event Types & Tags Basics

## Chpt3 – Search 1

### Creating an Eventtype

#### Manual

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

localhost:8000/en-GB/app/security\_4\_rookies/search?q=search%20index%3D"botsv1"%20sourcetype%3D"WinEventLog:Security"%20(EventCode%3D4624)

splunk>enterprise App: Security4Rookies

Search Datasets Reports Alerts Dashboards Ready Made Searches

New Search

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

✓ 3,209 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000) No Event Sampling

Events (3,209) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

List ▾ Format 20 Per Page ▾

Time	Event
24/08/2016 19:27:24.000	08/24/2016 11:27:24 AM LogName=Security SourceName=Microsoft Windows security

< Hide Fields All Fields i >

SELECTED FIELDS a host 3

splunk> turn data into doing

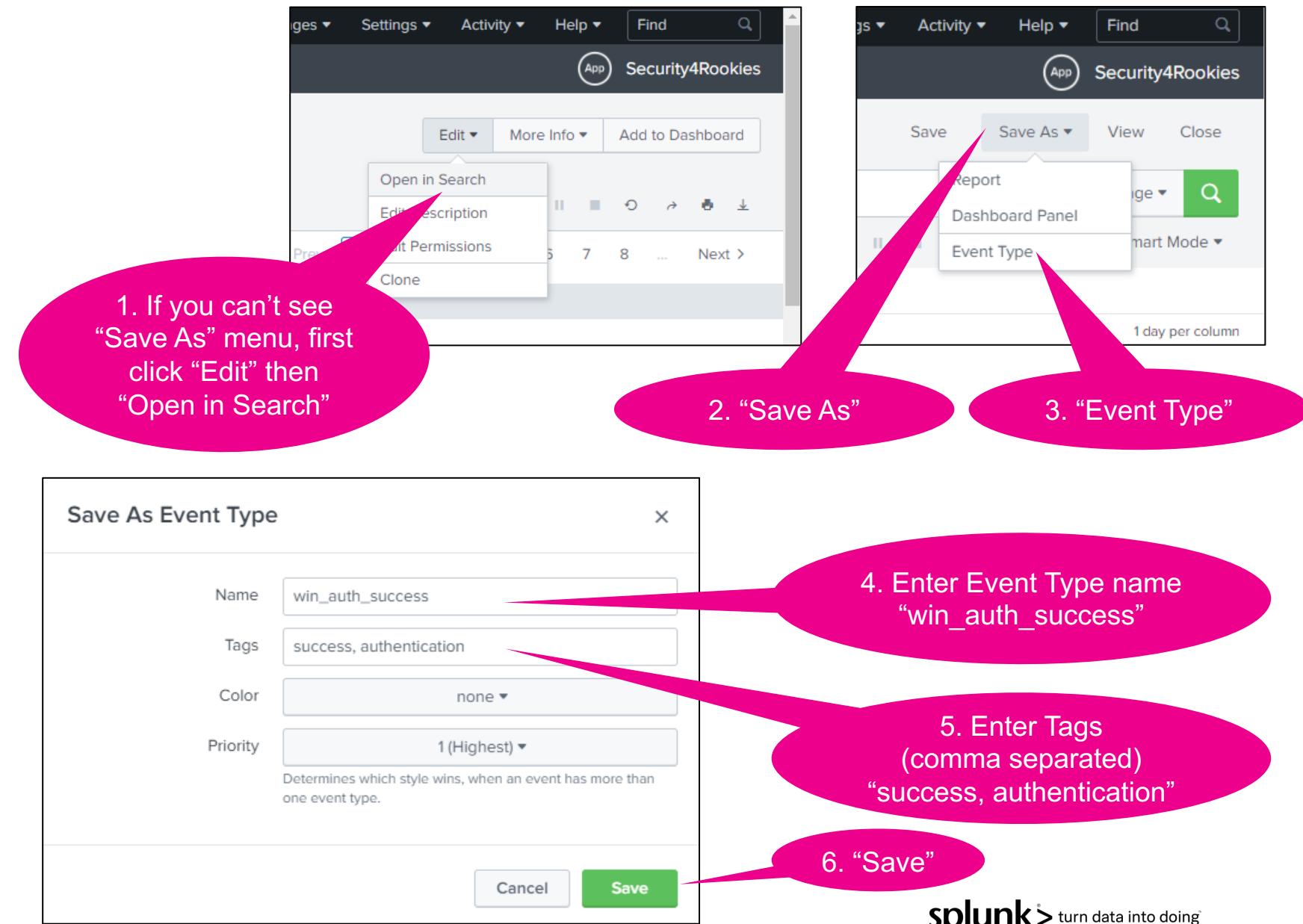
# Event Types & Tags Basics

## Chpt3 – Search 1

### Creating an Eventtype

#### Manual

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



# Event Types & Tags Basics

## Chpt3 – Search 2

### Searching by tags

#### Manual

tag=authentication tag=success

The screenshot shows the Splunk Enterprise search interface with the following details:

- Search Bar:** tag=authentication tag=success
- Results Summary:** 3,209 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000) No Event Sampling
- Event Types:** Events (3,209), Patterns, Statistics, Visualization
- Timeline:** Format Timeline ▾, Zoom Out, Zoom to Selection
- Event Preview:** Shows a single event with fields like Time, LogName, SourceName, EventCode, EventType, and a link to Show all 49 lines.
- Selected Fields:** host 3, source 1, sourcetype 1
- Interesting Fields:** Account\_Domain, Account\_Name, Authentication\_Package, ComputerName, EventCode, eventtype, EventType, Impersonation\_Level, index, Key\_Length, Keywords, linecount, LogName, Logon\_GUID
- Event Type Details:** A callout highlights the 'eventtype' field in the interesting fields list, with two steps:
  1. Click "eventtype"
  2. Note that our new Event Type is shown
- Event Type Statistics:** 1 Value, 100% of events, Top values, Events with this field, Values (win\_auth\_success: Count 3,209, % 100%), and filters for EventCode=4624 and EventType=0.

# Bonus Material

## Chpt3 – Search 3

### REGEX for the brave

#### Manual

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

localhost:8000/en-GB/app/security\_4\_rookies/search?q=search%20tag%3Dauthentication%20%

Apps Splunk Personal Research Articles React Python https://localhost:80... Okta

splunk>enterprise App: Security4Rookies ▾

Search Datasets Reports Alerts Dashboards Ready Made Searches ▾

New Search

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

✓ 413 events (10/08/2016 04:28:51.000 to 24.10.2016 19:27:44.000) No Event Sampling ▾

Events (413) Patterns Statistics

Format Timeline ▾ — Zoom Out

rex field=<field\_name> "(?P<>)"

rex field=<field\_name>
"beforepattern(?P<extract\_name>field\_match)afterpattern"

Time	Event
10/08/2016 22:48:05.858	{ [-] accept: text/html, application/xhtml+xml, accept_language: en-US ack_packets_in: 3 ack_packets_out: 4

< Hide Fields All Fields >

SELECTED FIELDS

a host 1  
a source 1  
a sourcetype 1

splunk> turn data into doing

# Plugging it all together

Where the rubber meets the road

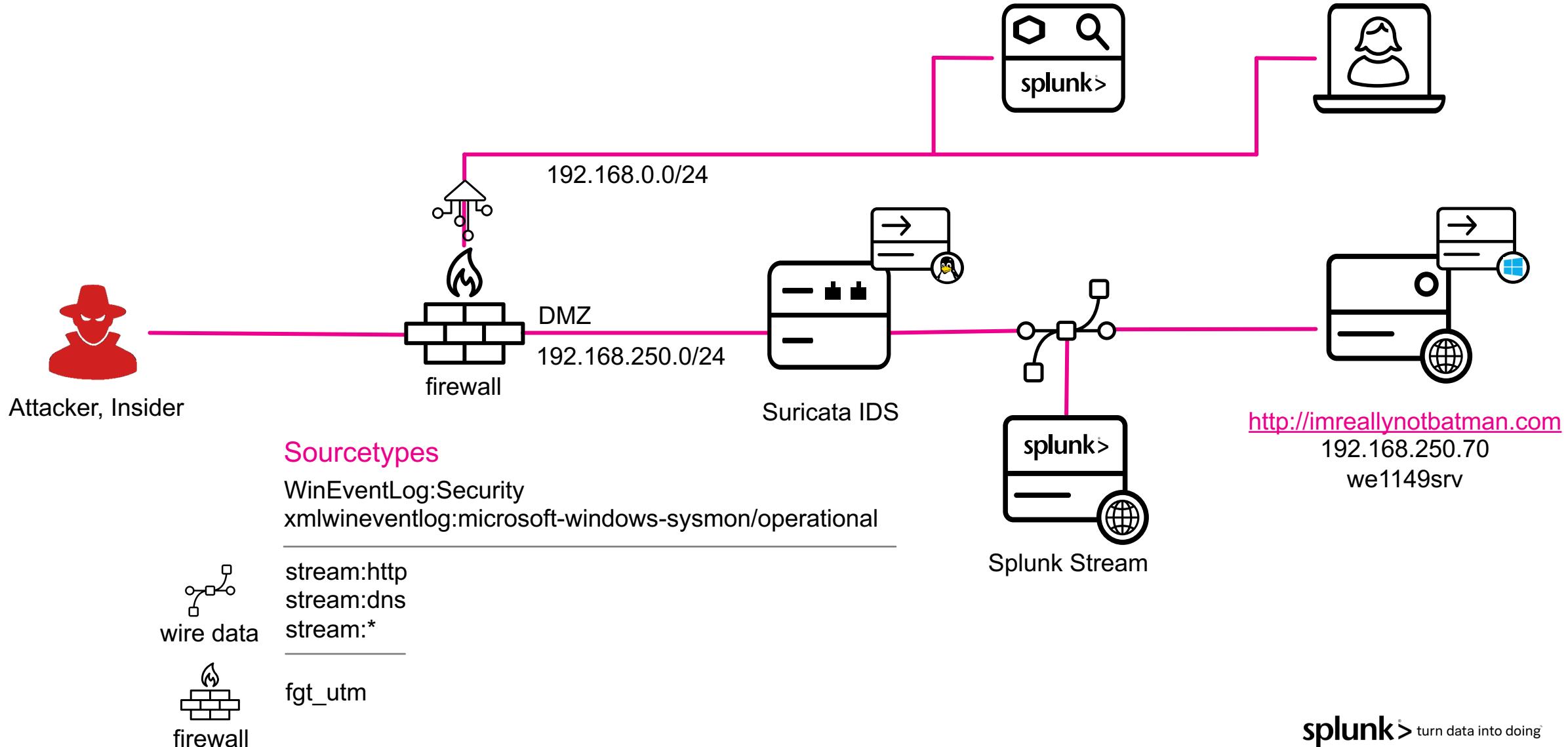
[imreallynotbatman.com](http://imreallynotbatman.com)

# Security Data and Searches

## For Security People



# WayneCorp Network



# Discovering the attack

## Chpt4 – Search 1

Filter traffic to the web server

### Manual

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

The screenshot shows the Splunk Enterprise search interface. The URL in the browser bar is `localhost:8000/en-GB/app/security_4_rookies/search?q=search%20`. The top navigation bar includes links for Apps, Splunk, Personal, Research Articles, React, Python, and https. The main header displays "splunk>enterprise" and "App: Security4Rookies". Below the header is a navigation bar with tabs for Search, Datasets, Reports, Alerts, Dashboards, and Ready Made Searches, where "Search" is currently selected. The main content area is titled "New Search". A search query is entered in the search bar: `index="botsv1" sourcetype=stream:http dest_ip=192.168.250.70`. Below the search bar, a message indicates `✓ 20,275 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000) No Event Samples`. Below this, there are four tabs: Events (20,275), Patterns, Statistics, and Visualization, with "Events (20,275)" being the active tab. At the bottom, there are controls for "Format Timeline" (with options for Zoom Out, Zoom to Selection, and Deselect), and a large green rectangular visualization area.

# 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
```

The screenshot shows the Splunk Enterprise search interface. The search bar contains the command: `index="botsv1" sourcetype=stream:http dest_ip=192.168.250.70 | stats count(src_ip) BY src_ip`. Below the search bar, it says "20,275 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000)". The "Statistics (3)" tab is selected. A pink callout points to the "src\_ip" dropdown under "Filter Statements" with the text "Aggregate & count". Another pink callout points to the "src\_ip" dropdown with the text "Filter Statements".

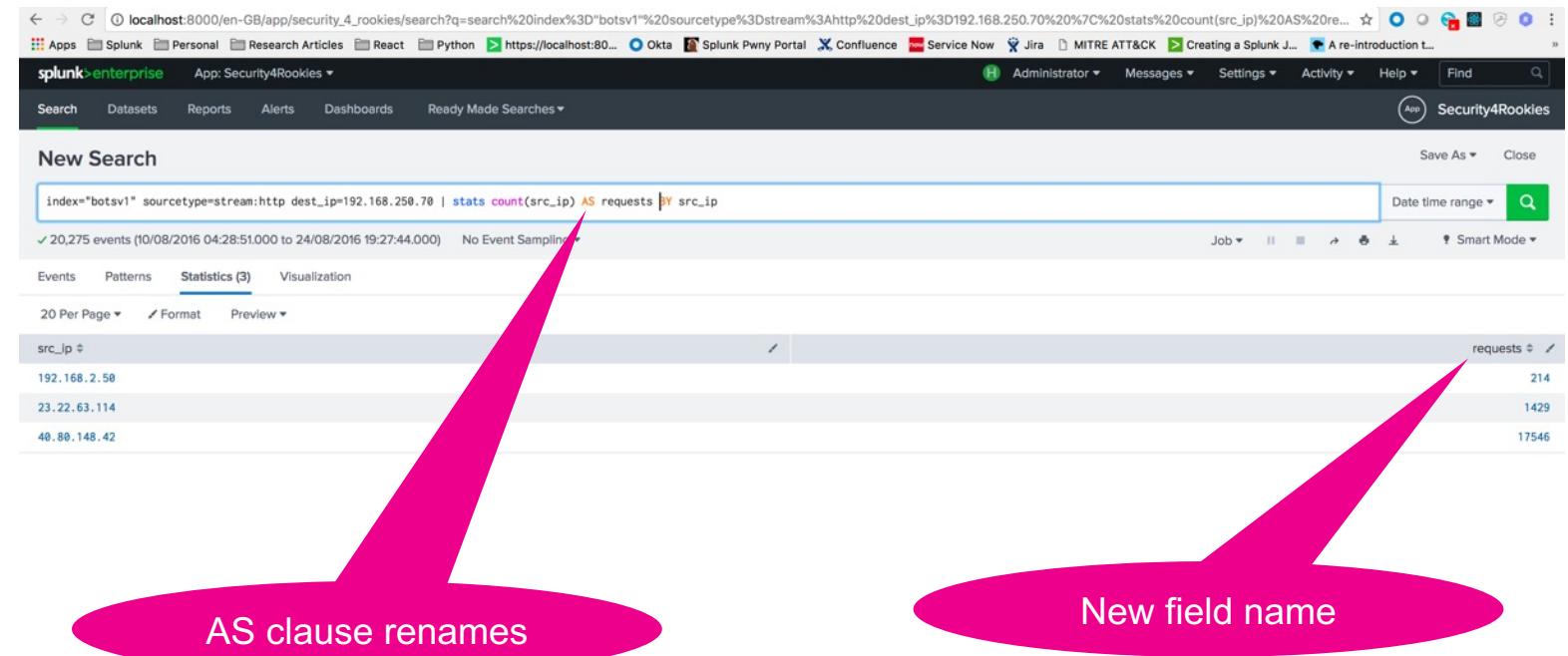
# Discovering the attack

## 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
```



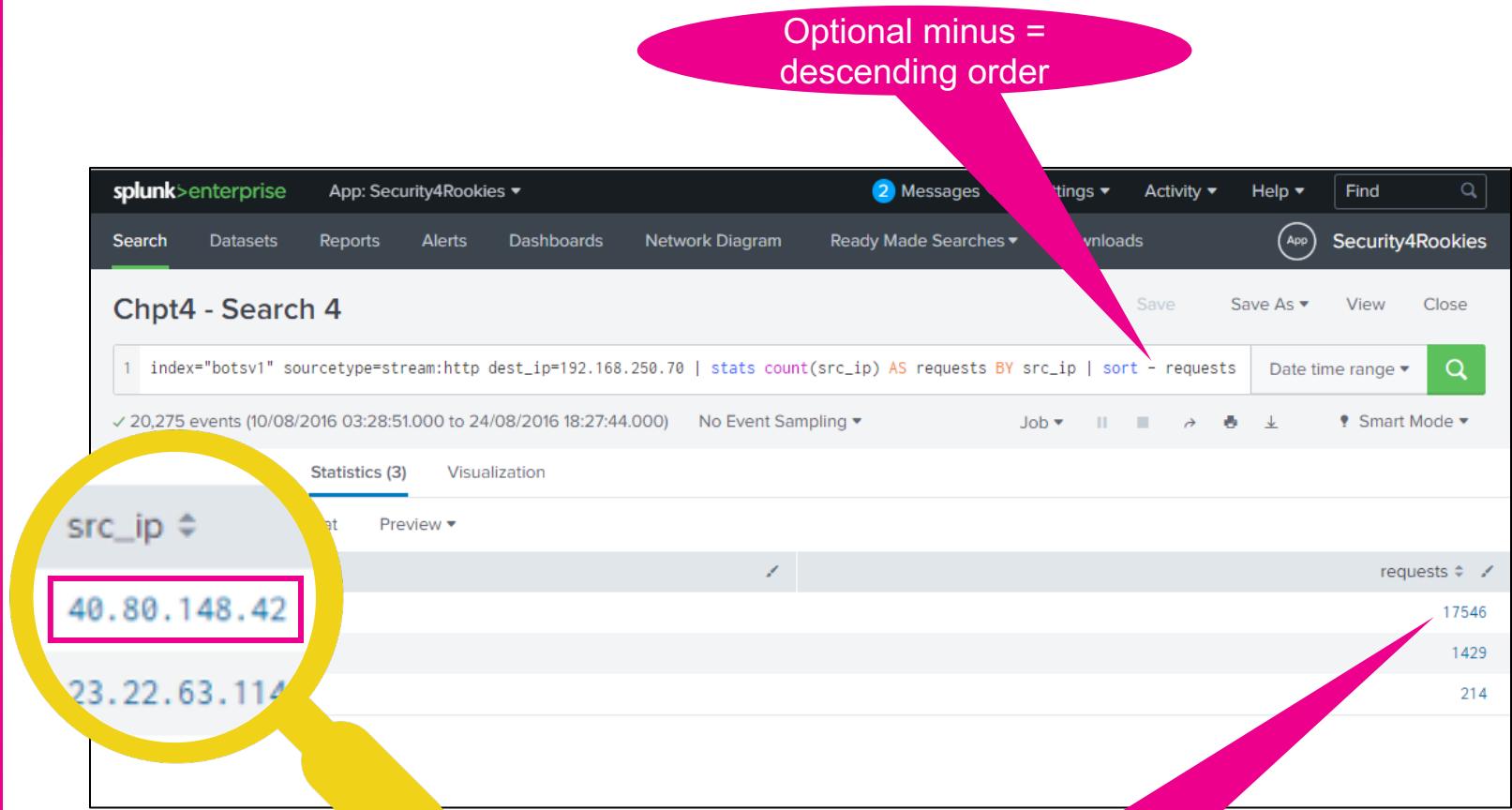
# Discovering the attack

## 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

splunk>enterprise App: Security4Rookies ▾

Search Datasets Reports Alerts Dashboards Network Diagram Ready Made Searches Downloads

2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

App Security4Rookies

**Chpt4 - Search 5**

1 index="botsv1" sourcetype=stream:http dest\_ip=192.168.250.70

✓ 20,275 events (10/08/2016 03:28:51.000 to 24/08/2016 18:27:44.000) No Events

Events (20,275) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

List ▾ Format 20 Per Page

< Hide Fields All Fields i Time Event

SELECTED FIELDS a host 1 a source 1 a sourcetype 1

INTERESTING FIELDS a accept 100+ # ack\_packets\_in 19 # ack\_packets\_out 13 # bytes 100+ # bytes\_in 100+ # bytes\_out 100+ a c\_ip 2 # bytes 93 a splunk\_server a src\_content 100 a src\_headers 100 a src\_ip a src\_mac a src\_port 100

Scroll down

src\_headers

>100 Values, 94.663% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values Count %

GET /joomla/administrator/index.php HTTP/1.1	412	2.147%
Accept-Encoding: identity Host: imreallynotbatman.com Connection: close User-Agent: Python-urllib/2.7		
GET / HTTP/1.1 Host: 192.168.250.70 Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1 Accept-Language: en Connection: Keep-Alive User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0) Pragma: no-cache Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, */*	88	0.458%
POST /joomla/index.php/component/search/ HTTP/1.1	88	0.458%
Content-Length: 121 Content-Type: application/x-www-form-urlencoded Referer: http://imreallynotbatman.com:80/ Cookie: ae72c62a4936b238523950a4f26f67d0=v7ikbsbiet3vph3 Host: imreallynotbatman.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Acunetix-Product: WVS/10.0 (Acunetix Web Vulnerability Scanner - Free Edition) Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm Accept: */*		

Acunetix Web Vulnerability Scanner

# 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
```

splunk>enterprise App: Security4Rookies ▾

2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

Search Datasets Reports Dashboards Network Diagram Ready Made Searches ▾ Downloads

App Security4Rookies

**Chpt4 - Search 6**

1 index="botsv1" sourcetype=stream:http dest\_ip=192.168.250.70 | stats count(src\_ip) AS requests BY src\_ip, http\_method | sort - requests

✓ 20,275 events (10/08/2016 03:28:51:000 to 24/08/2016 18:27:44.000) No Event Sampling ▾

Save Save As ▾ View Close

Events Patterns Statistics (9) Visualization

20 Per Page ▾ Format Preview ▾ Presentation last saved: Just now

src_ip	http_method	requests
40.80.148.42	POST	12844
40.80.148.42	GET	4678
23.22.63.114	GET	1017
23.22.63.114	POST	412
192.168.2.50	GET	213
40.80.148.42	OPTIONS	5
40.80.148.42	CONNECT	1
40.80.148.42	PROPFIND	1
40.80.148.42	TRACE	1

# 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
```

Chpt4 - Search 7

1 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

✓ 12,844 events (10/08/2016 03:28:51:000 to 24/08/2016 18:27:44.000) No Event Sampling ▾ Job ▾ II ▾ Smart Mode ▾

Events Patterns Statistics (8,612) Visualization

20 Per Page ▾ Format Preview ▾

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

form\_data ▾

&ordering=!(&&!|\*|\*|&searchphrase=all&searchword=&task=search  
&ordering=!(&&!|\*|\*|&searchphrase=all&searchword=e&task=search  
&ordering=!(&&!|\*|\*|&searchphrase=all&searchword=the&task=search  
&ordering=!(&&!|\*|\*|&searchphrase=any&searchword=&task=search  
&ordering=!(&&!|\*|\*|&searchphrase=exact&searchword=&task=search  
&ordering=!(&&!|\*|\*|&searchphrase=exact&searchword=the&task=search  
&ordering="+response.write(9006556\*9070592)+"&searchphrase=all&searchword=&task=search  
&ordering="+response.write(9141042\*9254568)+"&searchphrase=exact&searchword=the&task=search  
&ordering="+response.write(9248686\*9127579)+"&searchphrase=any&searchword=the&task=search  
&ordering="+response.write(9372747\*9029690)+"&searchphrase=any&searchword=&task=search  
&ordering="+response.write(9450103\*9133714)+"&searchphrase=exact&searchword=&task=search  
&ordering="+response.write(9508155\*9173884)+"&searchphrase=all&searchword=e&task=search  
&ordering="+response.write(9627406\*9035038)+"&searchphrase=all&searchword=the&task=search  
&ordering=";print(md5(acunetix\_wvs\_security\_test));\$a+"&searchphrase=all&searchword=e&task=search  
&ordering=";print(md5(acunetix\_wvs\_security\_test));\$a+"&searchphrase=all&searchword=the&task=search

# Discovering the attack

## Chpt4 – Search 8

### Investigating login activity

#### Manual

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

1 →

The screenshot shows the Splunk Enterprise search interface with the following details:

- Search Bar:** index="botsv1" sourcetype=stream:http http\_method="POST" form\_data=\*username\*passwd\*
- Results:** 413 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000) No Event Sampling
- Selected Fields:** Time, Event
- Event View:** Shows a single event from 10/08/2016 22:48:05.858 with fields like @version, @source, @sourcehost, @type, @index, @offset, @host, @file, @linecount, @location, @missing\_packets\_in, @missing\_packets\_out, @network\_interface, @packets\_in, @packets\_out, @punct, @reply\_time, @type, and @version.
- Field List:** A large list of available fields including date-related fields, destination fields, event type, form\_data, http-related fields, and network interface fields.
- Analysis Panel:**
  - form\_data:** Shows >100 Values, 100% of events.
  - Reports:** Top values, Top values by time, Events with this field.
  - Top 10 Values:**

	Count	%
username=admin&0960d493674eb04861bd64da9b662118=1	1	0.242%
&task=login&return=aW5kZXgucGhw&option=com_login&passwd=arthur	1	0.242%
username=admin&0edae02d7478dfb41641700ef384807a=1	1	0.242%
&task=login&return=aW5kZXgucGhw&option=com_login&passwd=bigdaddy	1	0.242%
username=admin&115c3aa6072f4b02b4354909431510f6=1	1	0.242%
&task=login&return=aW5kZXgucGhw&option=com_login&passwd=blazer	1	0.242%
username=admin&12c709bcc2e14d5a015f054d18d36537=1	1	0.242%
&task=login&return=aW5kZXgucGhw&option=com_login&passwd=fire	1	0.242%
username=admin&2a2ddf97716c1d1e9da21cdf82b231e=1	1	0.242%
&task=login&return=aW5kZXgucGhw&option=com_login&passwd=777777	1	0.242%
username=admin&2c340c4e46444ba249ff7e599e6dfa52=1	1	0.242%
&task=login&return=aW5kZXgucGhw&option=com_login&passwd=flower	1	0.242%
username=admin&32c15329bc3f78039869bb3bf17c28a6=1	1	0.242%
&task=login&return=aW5kZXgucGhw&option=com_login&	1	0.242%

A pink callout bubble points to the "form\_data" section of the analysis panel with the text: "Admin user being brute forced".

# 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"
```

The screenshot shows a Splunk search interface with the following details:

- Search Results:**
  - dest\_ip: 192.168.250.70
  - dest\_mac: 00:0C:29:C4:02:7E
  - dest\_port: 80
  - duplicate\_packets\_in: 1
- Selected Fields:** A dropdown menu shows "form\_data" is selected. Other options include dest\_ip, dest\_mac, dest\_port, and duplicate\_packets\_in.
- Reports:**
  - Top values:** Shows "username=admin&passwd=batman&option=com\_login&task=login&return=aW5kZXgucGhw&45ec827a3f67ce0efc546d81f7356acc=1" with a count of 1 and 100%.
  - Top values by time:** Shows "request: POST /joomla/administrator/index.php HTTP/1.1" with a count of 5 and 100%.
  - Rare values:** Shows "request\_ack\_time: 51724" and "request\_time: 0".
- Events with this field:** Shows a single event with the following fields and values:
 

	Count	%
username=admin&passwd=batman&option=com_login&task=login&return=aW5kZXgucGhw&45ec827a3f67ce0efc546d81f7356acc=1	1	100%
- Values:** Shows the same event with the following breakdown:
 

	Count	%
username=admin&passwd=batman&option=com_login&task=login&return=aW5kZXgucGhw&45ec827a3f67ce0efc546d81f7356acc=1	1	100%

Successful Login

# Unauthorized Access 😞

What happened next

# Post Exploit

## Setting the time range

The screenshot shows the Splunk search interface with the following details:

- Time Range:** The time range is set to "After this time" (highlighted by a pink box and arrow 1). The specific time is 10/08/2016 21:48:05.858.
- Event Preview:** The event details are displayed on the right, including:
  - accept: text/html, application/xhtml+xml, \*/\*
  - \_time: 2016-10-08T21:48:05.858Z
  - client\_ip: 192.168.1.10
  - client\_rtt\_sum: 82195
  - connection\_type: Keep-Alive
  - cookie: 7598a3465c906161e060ac551a9e0276=9qfk2
  - cs\_cache\_control: no-cache
  - cs\_content\_length: 111
  - cs\_content\_type: application/x-www-form-urlencoded
  - cs\_version: [ [+]
- Nearby Events:** A search for nearby events within 5 seconds is applied.

# 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
```

New Search

index=botsv1 sourcetype="stream:http" dest\_ip=192.168.250.70 http\_method="POST" \*.exe

1 event (10/08/2016 22:48:05.000 to 04/09/2018 11:54:48.000) No Event Sampling ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection Deselect

1 month per column

	Time	Event
< Hide Fields	All Fields	10/08/2016 22:52:47.035 {"endtime": "2016-08-10T21:52:47.035552", "timestamp": "2016-08-10T21:52:45.4374452", "accept": "text/html, application/xhtml+xml, */*", "accept_language": "en-US", "cache_control": "no-cache", "connection": "close", "content_length": "94", "content_type": "application/x-www-form-urlencoded", "host": "192.168.250.70", "http_method": "POST", "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36", "x_forwarded_for": "192.168.250.70", "x_forwarded_proto": "http", "x_originating_ip": "192.168.250.70", "x_real_ip": "192.168.250.70", "x_served_by": "nginx/1.13.10"} <b>his program cannot be run in DOS mode</b>

List ▾ Format 20 Per Page ▾

SELECTED FIELDS  
*a host 1*  
*a source 1*  
*a sourcetype 1*

Executable uploaded

# 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
```

splunk>enterprise App: Security4Rookies ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Datasets Reports Alerts Dashboards Ready Made Searches ▾

New Search

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

✓ 98 events (10/08/2016 22:48:00.000 to 04/09/2018 12:07:37.000) No Event Sampling ▾

Events Patterns Statistics (98) Visualization

20 Per Page ▾ Format Preview ▾

\_time ▾ parent\_process ▾ cmdline ▾

_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&gt;&lt;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&gt;&lt;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&gt;&lt;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&gt;&lt;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&gt;&lt;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&gt;&lt;1"
2016-09-10 22:20:22	C:\Windows\SysWOW64\cmd.exe	\??\C:\Windows\system32\conhost.exe 0xffffffff

Imnotbatman.jpg  
overwritten!

# Post Exploit

## Chpt5 – Search 3

### Investigating Web Server Activity

#### Manual

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

**splunk>enterprise** App: Security4Rookies ▾

Search Datasets Reports Alerts Dashboards Ready Made Searches ▾

### New Search

index=botsv1 sourcetype="stream:http" http\_method="GET" src\_ip=192.168.250.70

✓ 7 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000) No Event Sampling ▾

	Events (7)	Patterns	Statistics	Visualization																		
Format Timeline ▾		<ul style="list-style-type: none"> <li>a http_content_type 1</li> <li>a http_method 1</li> <li>a index 1</li> <li># linecount 1</li> <li># missing_packets_in 1</li> <li># missing_packets_out 1</li> <li>a network_interface 1</li> <li># packets_in 2</li> <li># packets_out 2</li> <li>a punct 2</li> <li># reply_time 6</li> <li>a request 4</li> <li># request_ack_time 7</li> <li># request_time 3</li> <li># response_ack_time 5</li> <li># response_time 3</li> <li>cache_control 1</li> </ul>	<p>src_ip: 192.168.250.70 src_mac: 00:0C:29:C4:02:7E src_port: 63139</p> <p><b>request</b> 4 Values, 100% of events</p> <p><b>Reports</b> Top values Top values by time Rare values Events with this field</p> <table border="1"> <thead> <tr> <th>Values</th> <th>Count</th> <th>%</th> </tr> </thead> <tbody> <tr> <td>GET /core/list.xml HTTP/1.1</td> <td>2</td> <td>28.571%</td> </tr> <tr> <td>GET /jed/list.xml HTTP/1.1</td> <td>2</td> <td>28.571%</td> </tr> <tr> <td>GET /poisonivy-is-coming-for-you-batman.jpeg</td> <td>2</td> <td>28.571%</td> </tr> <tr> <td>HTTP/1.1</td> <td></td> <td></td> </tr> <tr> <td>/core/extensions/com_joomlaupdate.xml</td> <td>1</td> <td>14.286%</td> </tr> </tbody> </table> <p>client_rtt: 202 client_rtt_packets: 1 client_rtt_sum: 202 cs_version: 1.0 data_center: 0</p>	Values	Count	%	GET /core/list.xml HTTP/1.1	2	28.571%	GET /jed/list.xml HTTP/1.1	2	28.571%	GET /poisonivy-is-coming-for-you-batman.jpeg	2	28.571%	HTTP/1.1			/core/extensions/com_joomlaupdate.xml	1	14.286%	<p><b>More Badness!</b></p> <p>1</p>
Values	Count	%																				
GET /core/list.xml HTTP/1.1	2	28.571%																				
GET /jed/list.xml HTTP/1.1	2	28.571%																				
GET /poisonivy-is-coming-for-you-batman.jpeg	2	28.571%																				
HTTP/1.1																						
/core/extensions/com_joomlaupdate.xml	1	14.286%																				

**splunk> turn data into doing**

# Post Exploit

## Chpt5 – Search 3

### Investigating Web Server Activity

#### Manual

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

	Event
a c_ip 1	cc_version: 1.0
# canceled 1	data_center_time: 0
a capture_hostname 1	data_packets_in: 2
# client_rtt 2	data_packets_out: 0
# client_rtt_packets 1	dest_ip: 23.22.63.114
# client_rtt_sum 2	dest_mac: 08:5B:0E:93:92:AF
# cs_version 1	dest_port: 1337
# data_center_time 1	duplicate_packets_in: 2
# data_packets_in 1	duplicate_packets_out: 0
# data_packets_out 1	endtime: 2016-08-10T22:13:46.915172Z
# date_hour 1	http_method: GET
# date_mday 1	missing_packets_in: 0
# date_minute 2	missing_packets_out: 0
a date_month 1	network_interface: eth1
# date_second 2	packets_in: 6
a date_wday 1	packets_out: 5
# date_year 1	reply_time: 0
# date_zone 1	request: GET /poisonivy-is-coming-for-you-batman.jpeg HTTP/1.0
a dest_ip 1	request_ack_time: 3246
a dest_mac 1	request_time: 61714
# dest_port 1	response_ack_time: 0
# duplicate_packets_in 1	response_time: 0
# duplicate_packets_out 1	server_rtt: 32357
a endtime 2	server_rtt_packets: 2
a http_method 1	server_rtt_sum: 64714
a index 1	site: prankglassinebracket.jumpingcrab.com:1337
# linecount 1	src_headers: GET /poisonivy-is-coming-for-you-batman.jpeg HTTP/1.0
# missing_packets_in 1	Host: prankglassinebracket.jumpingcrab.com:1337
# missing_packets_out 1	
a network_interface 1	

Fetching jpeg

DDNS Site

# 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
```

The screenshot shows the Splunk interface with the following steps highlighted:

1. A pink arrow points from the top right corner of the main search results area to the "Save As" dropdown menu in the top right corner of the window.
2. A pink arrow points from the "Save As" dropdown menu to the "Dashboard Panel" option.
3. A pink arrow points from the "Dashboard" field to the "New" button.
4. A pink arrow points from the "Dashboard Title" field to the value "Security Operations".
5. A pink arrow points from the "Dashboard ID" field to the value "security\_operations".
6. A pink arrow points from the "Panel Title" field to the value "Password attempts per user".
7. A pink arrow points from the "Save" button at the bottom right of the dialog to the "splunk" logo in the bottom right corner of the page.

**Save As Dashboard Panel**

Dashboard: New

Dashboard Title: Security Operations

Dashboard ID: security\_operations

Dashboard Description: My First Dashboard

Dashboard Permissions: Private Shared in App

Panel Title: Password attempts per user

Panel Powered By:  Inline Search  Report

Drilldown: No action

Panel Content: Statistics Table

Cancel Save

**splunk** turn data into doing

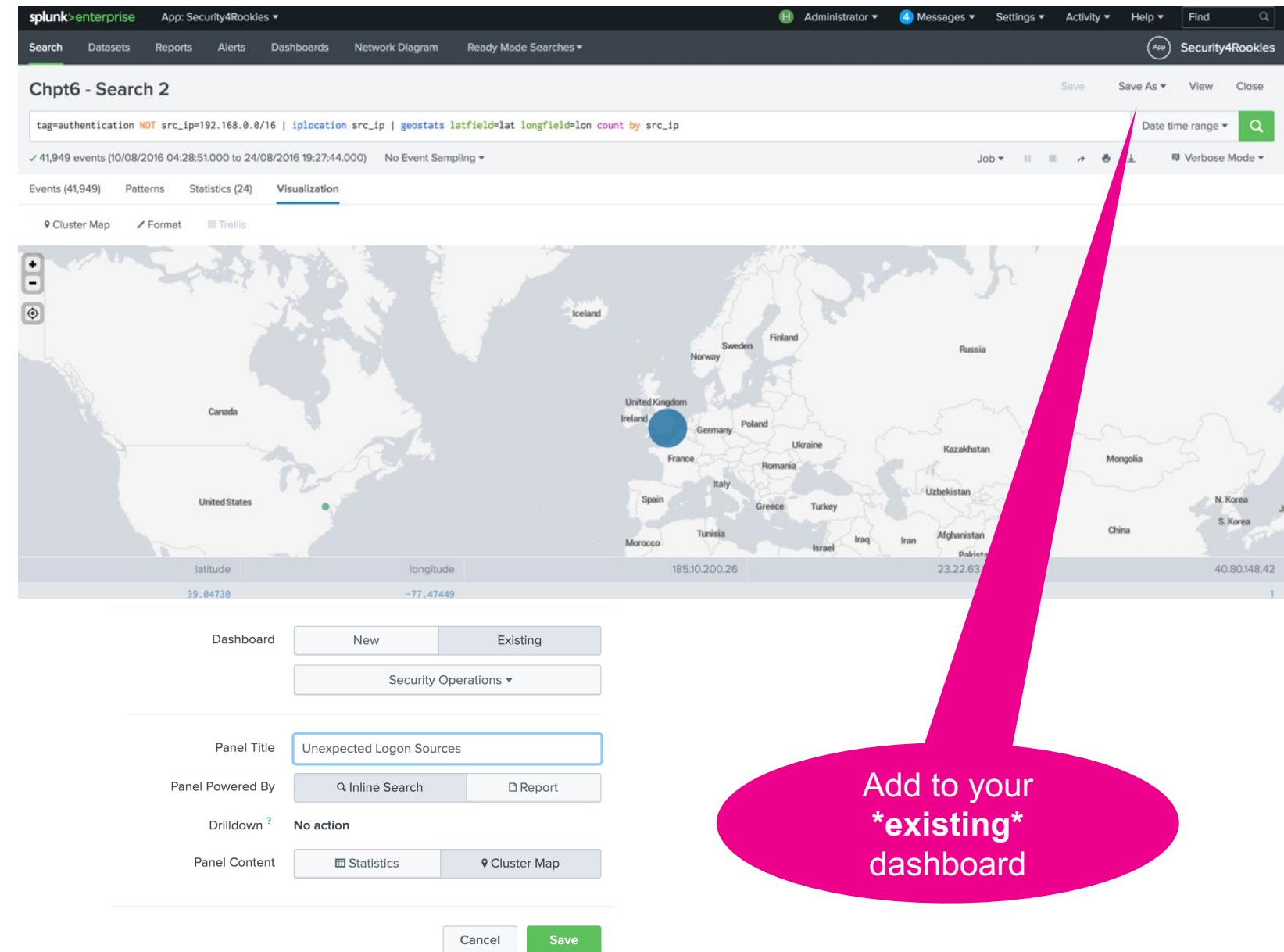
# Dashboards

## 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
```

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** 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
- Results Summary:** 23,936 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000) No Event Sampling
- Panel Tabs:** Events (23,936), Patterns, Statistics (247) (selected), Visualization
- Statistics View:** Shows a table of user agent names and their lengths. The table includes columns for count and ua\_len.

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
Nessus	33	6
@@NxfDt	1	7
fN7g9VL6	1	8

Add to your existing dashboard

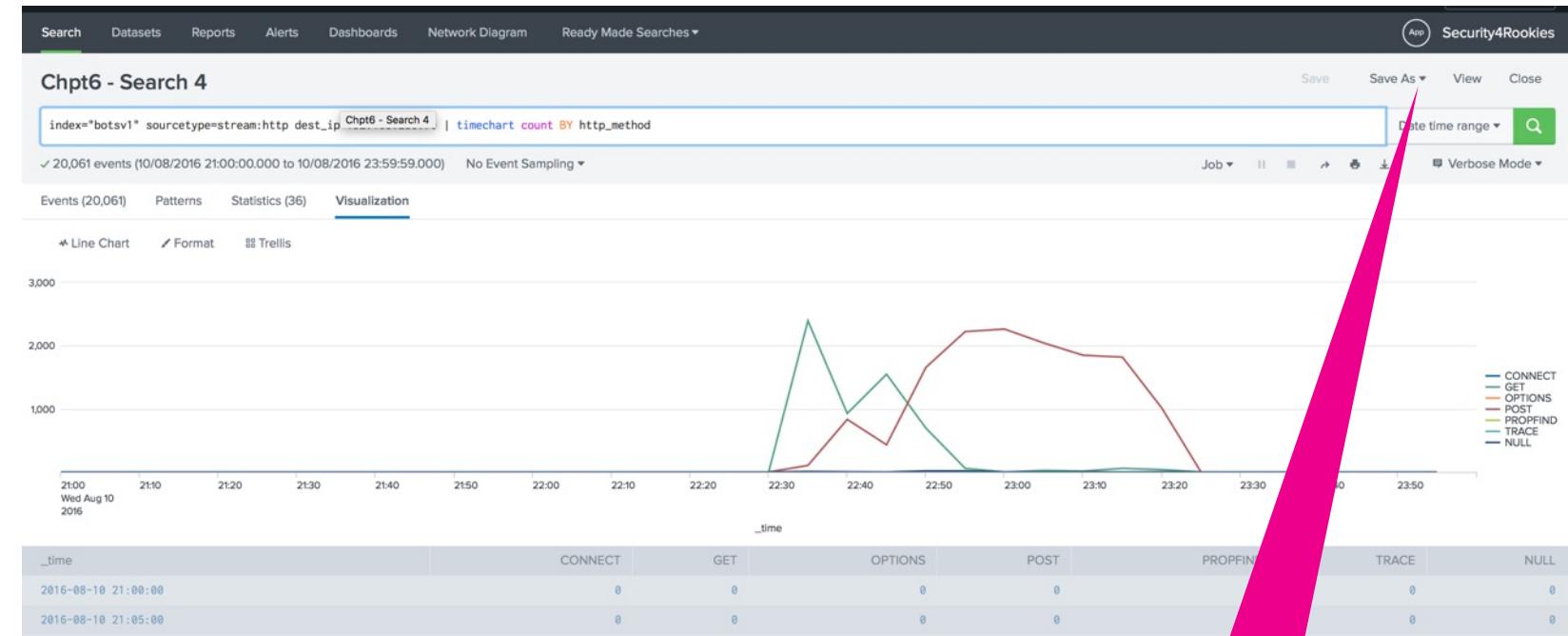
# Dashboards

## 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

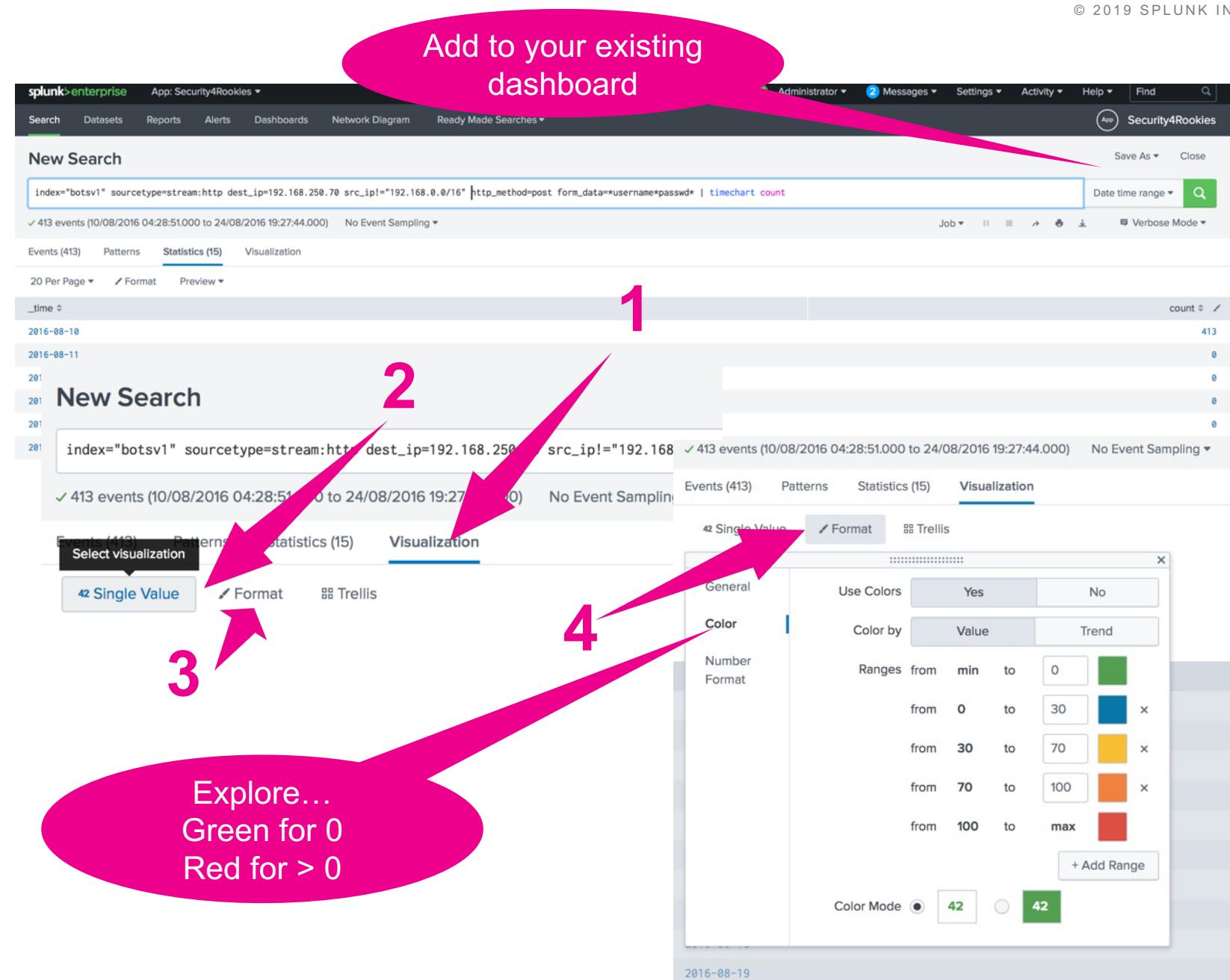
# Dashboards

# 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
```



# 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
```

Add to your existing dashboard

New Search

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

✓ 13,394 events (10/08/2016 04:28:51.000 to 11/08/2016 19:27:44.000) No Event Sampling ▾

Events (13,394) Patterns Statistics (79) **Visualization**

42 Single Value Format Trellis

**1**

**2**

**3**

New Search

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

✓ 13,394 events (10/08/2016 04:28:51.000 to 11/08/2016 19:27:44.000) No Event Sampling ▾

Events (13,394) Patterns Statistics (79) **Visualization**

42 Single Value Format Trellis

General Use Colors Yes No

Color Color by Value Trend

Ranges from min to 0 from 0 to max + Add Range

Number Format

Color Mode 42 42

Explore... Green for 0 Red for > 0

# Dashboards

Visualizations

Interactive

The screenshot shows the Splunk Enterprise interface with the following elements:

- Header:** splunk>enterprise App: Security4Rookies ▾
- Top Navigation:** Search, Datasets, Reports, Alerts, Dashboards, Network Diagram, Ready M...
- Search Results:** Dashboards
  - Dashboard icon: ent
  - Title: Dashboards
  - Description: Dashboards include searches, visualizations, and inp...
  - No E 2 Dashboards
  - List:
    - i Title ▾
    - > Network Diagram
    - > Security Operations
- Details View:** Security Operations
  - Section: Password attempts per user
  - Host: host ▾ splunk-02
  - User: user ▾ admin
  - Count: numPasswords ▾ 344
- Bottom Header:** Search, Datasets, Reports, Alerts, Dashboards, Network Diagram, Ready Made Searches ▾, Security4Rookies, Edit, Export ▾, ...

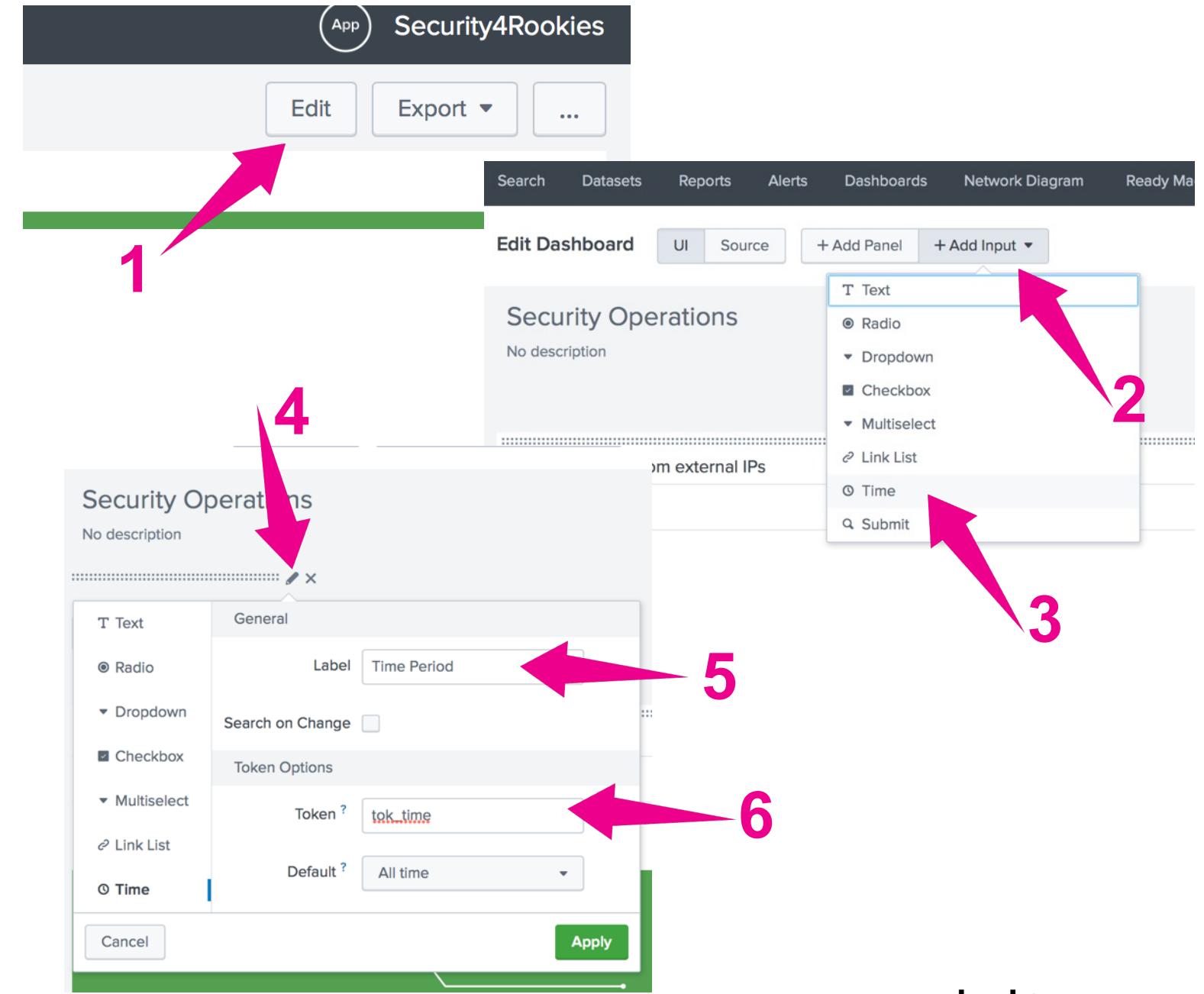
Three pink arrows point to specific areas:

- Points to the "Dashboards" tab in the top navigation bar.
- Points to the "Security Operations" dashboard in the search results list.
- Points to the "Security4Rookies" app icon in the bottom header.

# Dashboards

## Visualizations

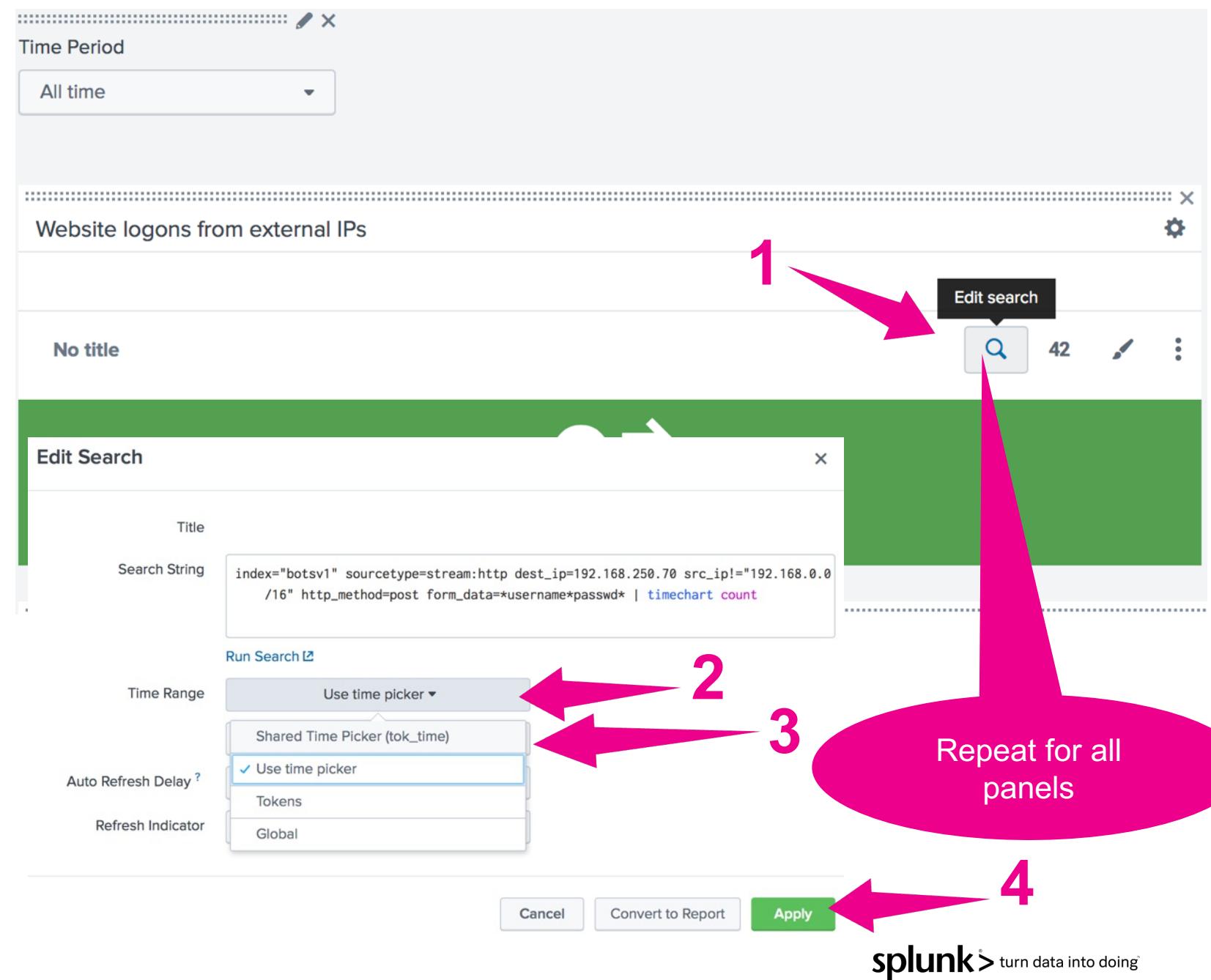
### Add time selector



# Dashboards

## Visualizations

Make panels react



# Dashboards

## Visualizations

### Changing Visualization Type

The screenshot shows the Splunk Visualization editor interface. At the top, there is a table titled "Password attempts per user" with several columns and rows of data. A pink arrow labeled "1" points to the "stacked 100%" button in the top right corner of the visualization panel.

In the center, a modal window titled "Splunk Visualizations" displays various visualization types: Line, Heatmap, Area, Bar, Scatter, Pie, Gauge, Map, and a search bar. A pink arrow labeled "2" points to the "Bar" icon, which is selected. Below this, a "Find more visualizations" link is visible.

At the bottom, a "Column Chart" panel is open, showing a stacked bar chart with multiple colored segments. To the right of the chart are several configuration options:

- General**: Stack Mode dropdown set to "stacked 100%" (highlighted with a blue border).
- Stack Mode**: Buttons for "Stacked" and "Unstacked".
- Multi-series Mode**: Buttons for "Yes" and "No".
- Show Data Values**: Buttons for "Off", "On", and "Min/Max".
- Legend**: A legend panel showing color-coded squares for each data series.

# Dashboards

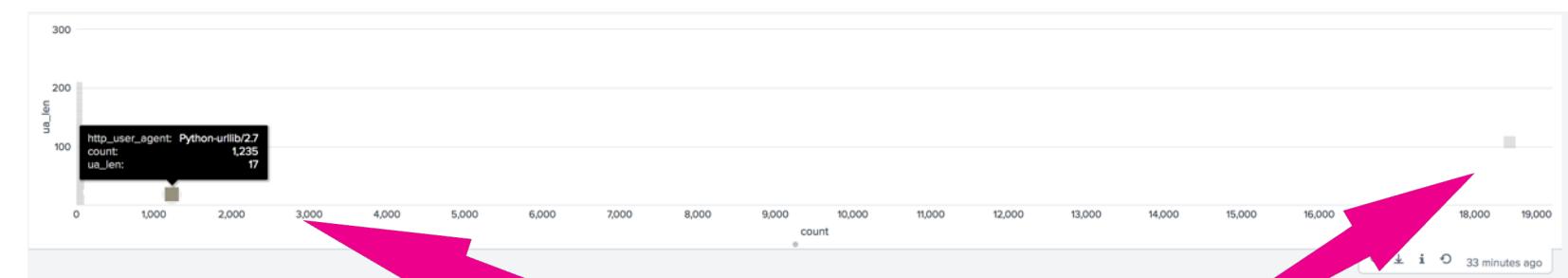
## Visualizations

### 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

YUK! – Wrong type of vis for the data!

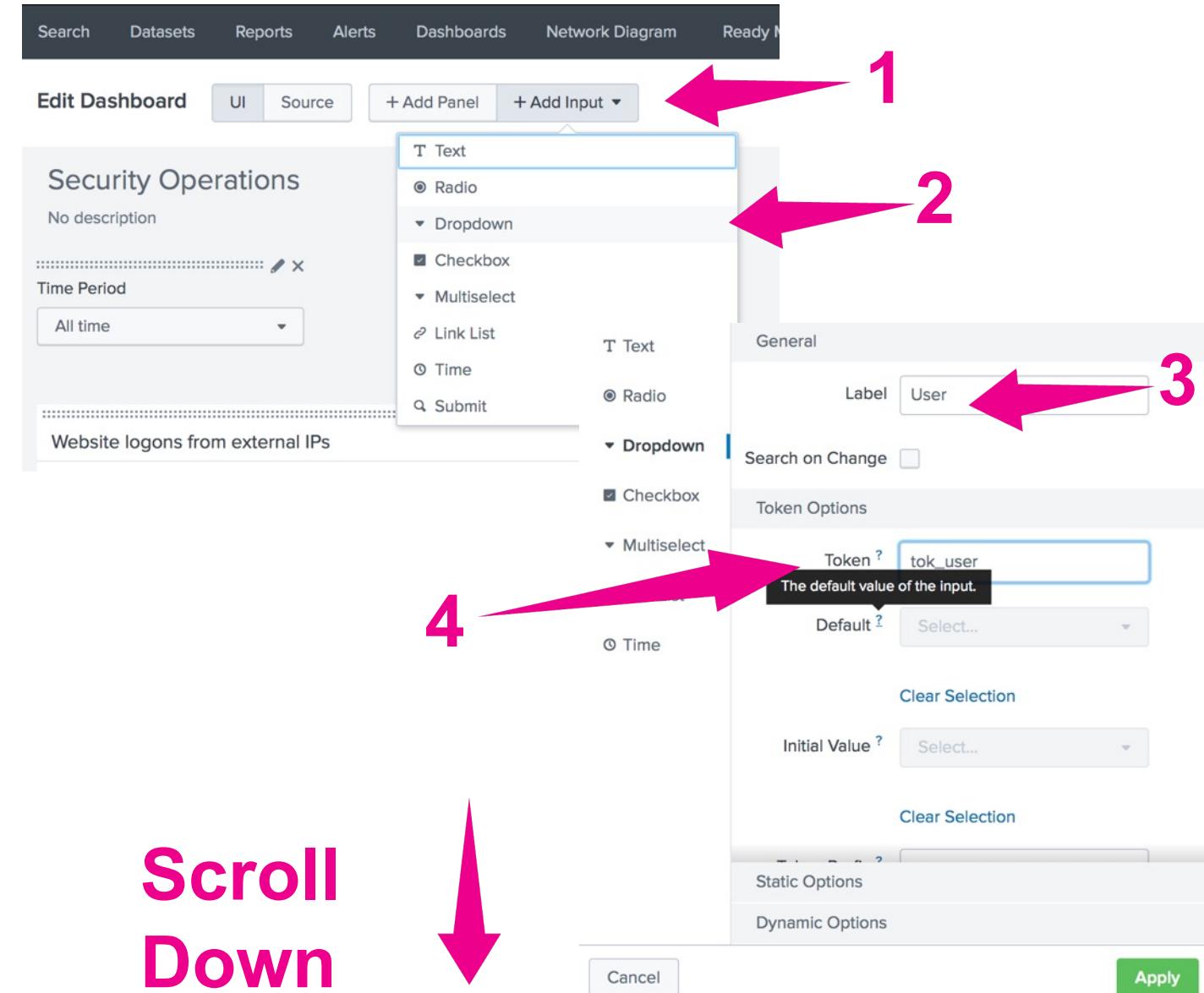


Rare features stand out with good visualizations

# Dashboards

## Visualizations

### Interactive Filtering



Scroll  
Down

# Dashboards

## Visualizations

Continued

Static Options

Name	Value
ALL	*

+ Add New

Dynamic Options

Content Type

Search String

Run Search [Run Search ↗](#)

Last 24 hours

Field For Label

Field For Value

7

8

NOT YET!

Apply

5

6

7

8

NOT YET!

# Dashboards

## Visualizations

Continued

Token Options

Token ? `tok_user`

Default ? ALL

Clear Selection

Initial Value ? ALL

Clear Selection

Token Prefix ?

**Scroll Back Up!**

9

10

11

T Text  
Radio  
Dropdown  
Checkbox  
Multiselect  
Link List  
Time

General  
Token Options  
Static Options  
+ Add New  
Dynamic Options  
Content Type   
Search String   
Run Search

Last 24 hours

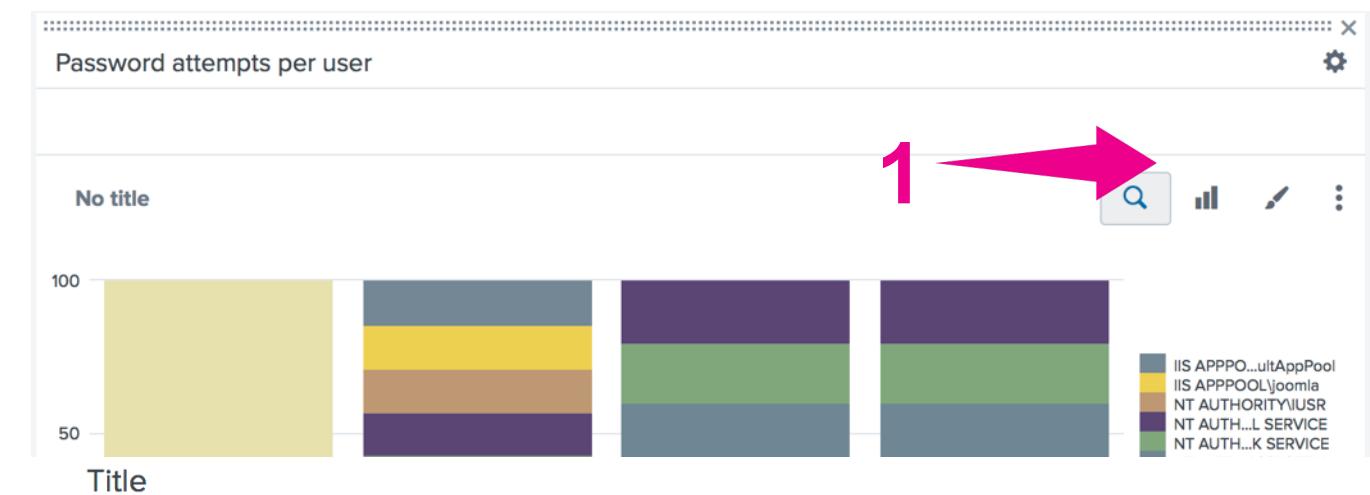
Field For Label ?   
Field For Value ?

CANCEL  Apply

# 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
```

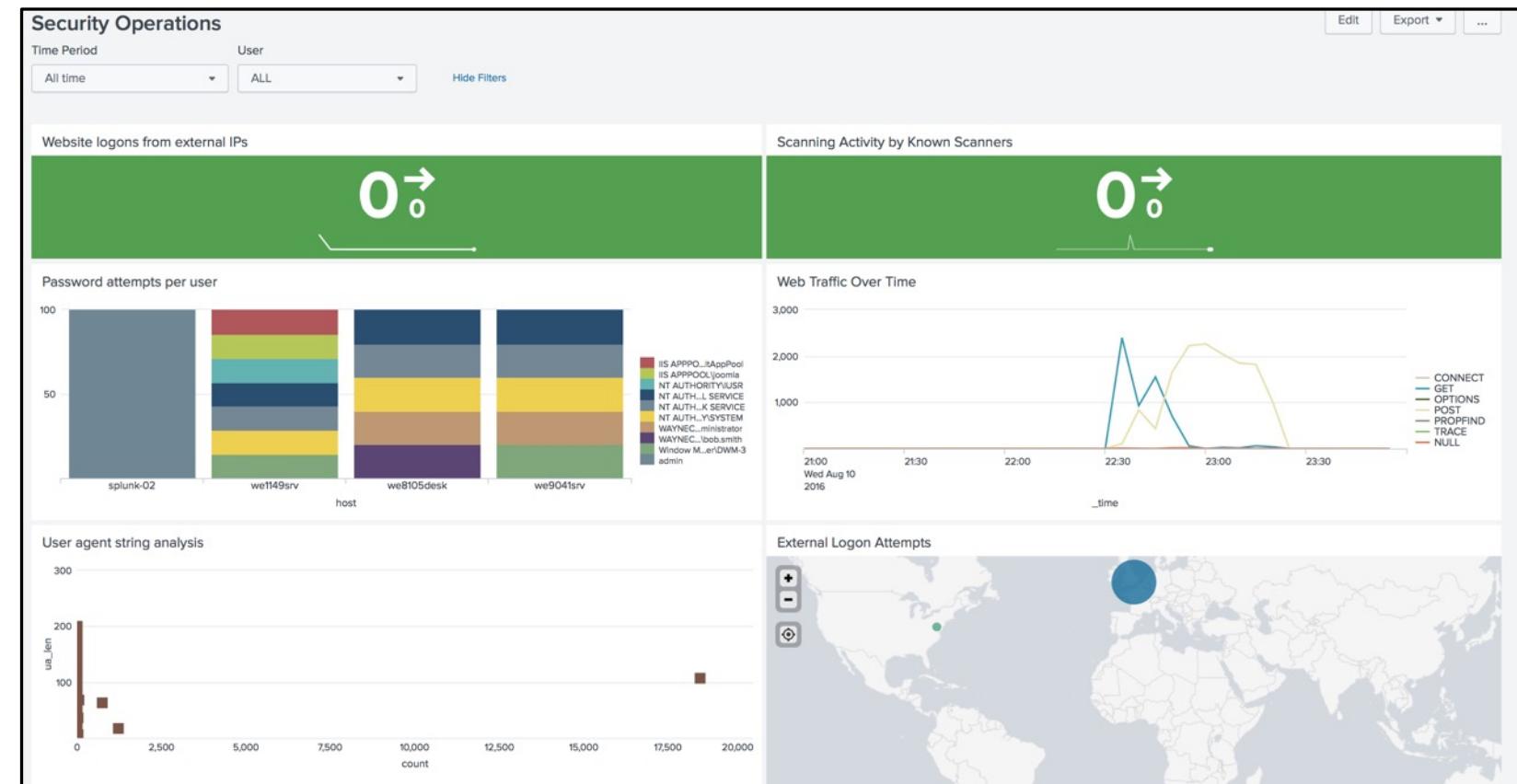
Run Search ↗

ADD  
“search user=\$tok\_user\$ |”

# Dashboards

## Dashboard Hero

# And.... Breathe!



# 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](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

splunk>

# SPLUNK SECURITY DATASET PROJECT

Registration

The Splunk Security Dataset Project will provide access to Splunk customers, external security researchers, and thought leaders to an ever growing collection of exciting datasets. Every participant will be able to access real data in Splunk hosted portal and explore/analyze various datasets with an educational tutorial. Each dataset will be given an educational tutorial and a walk through of the data along with full access to search the data!

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

The Splunk Security Dataset Project will provide access to Splunk customers, external security researchers, and thought leaders to an ever growing collection of exciting datasets. Every participant will be able to access real data in Splunk hosted portal and explore/analyze various datasets with an educational tutorial. Each dataset will be given an educational tutorial and a walk through of the data along with full access to search the data!

splunk> App: I... Splunk Messages Settings Activity Help Find

Overview Web-Shells Supplemental Material Search Investigating MACCDC

Introduction

Investigating the MACCDC Dataset

Welcome to Investigating the MACCDC 2012 Dataset!

This workshop is designed to provide a very brief hands-on walk through using Splunk as an investigative tool against the dataset captured during the Mid-Atlantic Collegiate Cyber Defense Competition in 2012. For those of you unfamiliar with MACCDC, this is an event where professional red teamers attack a network protected by college students in blue team roles. The dataset is captured with PCAP and then was converted to Bro by Mike Sconzo. He also ran the PCAPs against Snort IDS and

### Interested?

Sign up now to receive immediate access and alerts to notifications about new additions to the Splunk Security Dataset Project

Email Address: \*

First Name: \*

Last Name: \*

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

# Todays Content

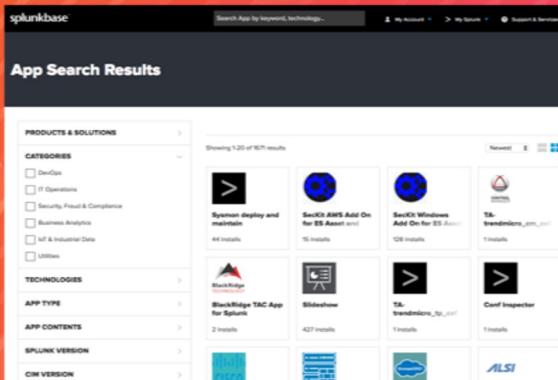
## Download and play

The screenshot shows a Splunk web interface with a dark header bar. In the top right, there are links for "Research Articles", "React", "Python", "https://localhost:8...", "Okta", "Splunk Pwny Portal", and "Cor". Below the header is a navigation bar with tabs: "Alerts", "Dashboards", "Network Diagram", "Ready Made Searches", and "Downloads". The "Downloads" tab is highlighted with a green underline. The main content area displays two items:

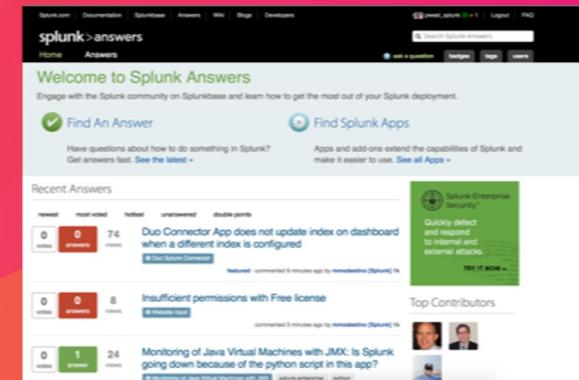
- A link to a "Powerpoint presentation presented today".
- A link to a "Security 4 Rookies app, to install on your phone please Download from here." This link is circled in red and has a pink arrow pointing to it from the bottom left.

# Thriving Community

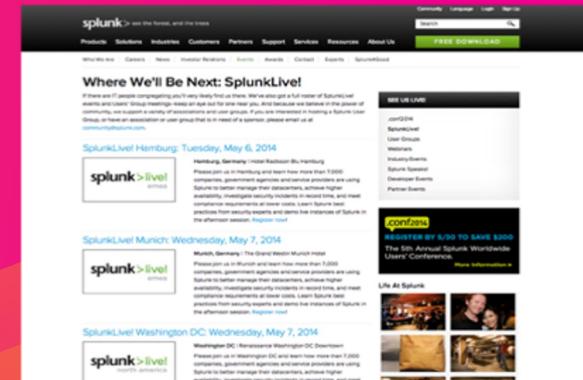
## Splunkbase



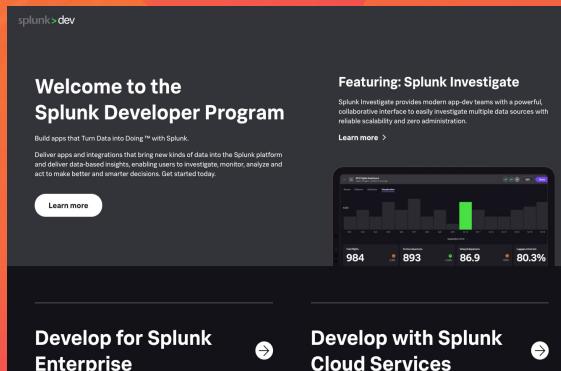
## Splunk Answers



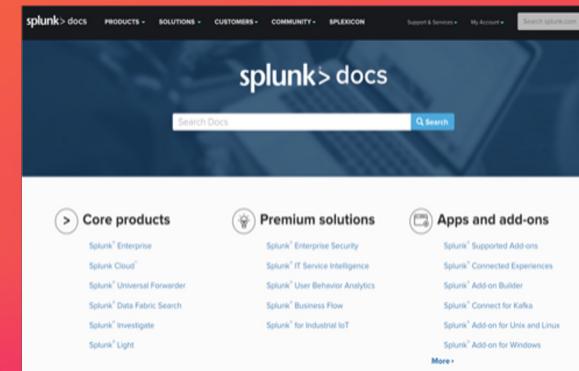
## Splunk Events



## Developer Resources



## Documentation



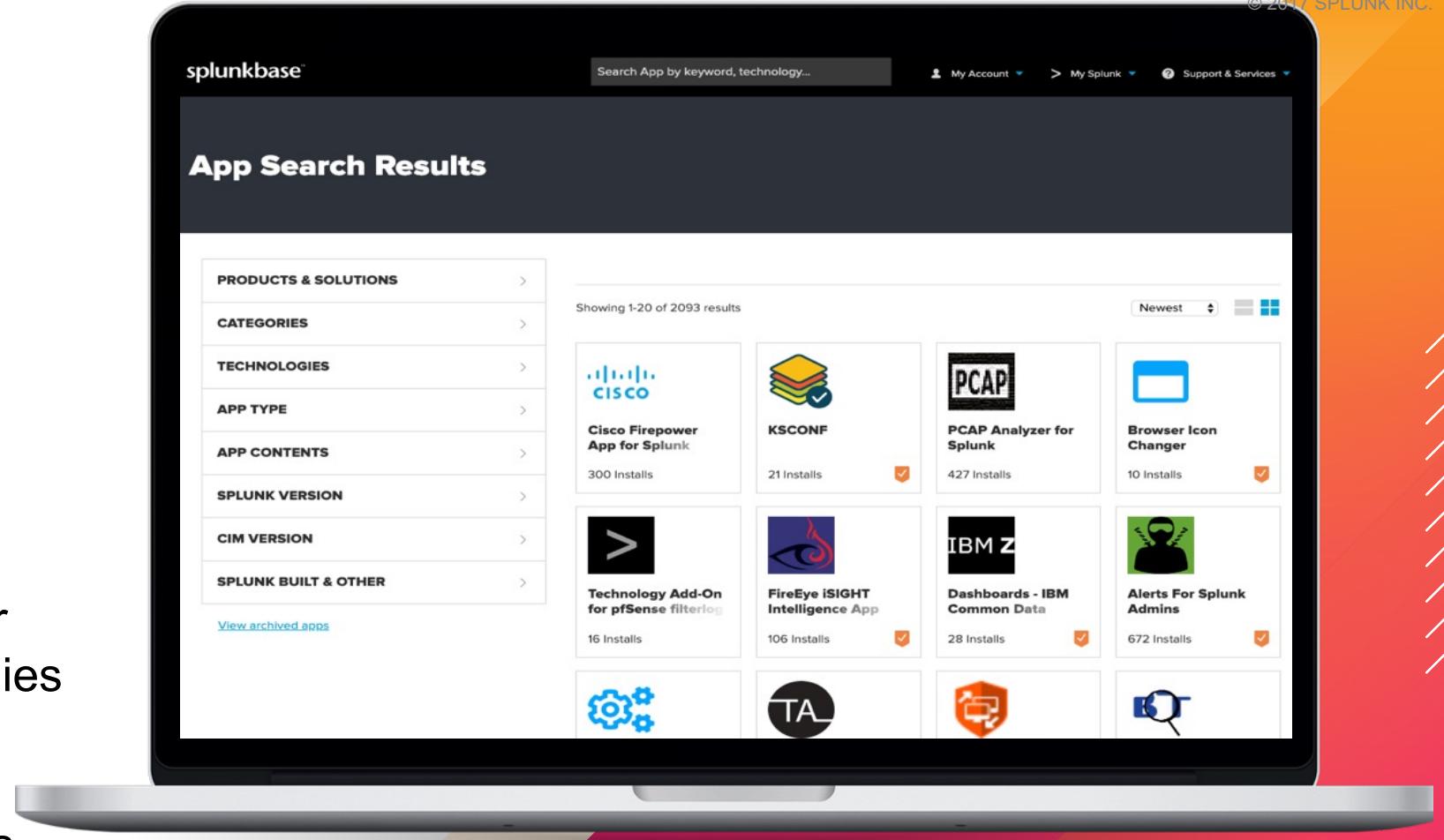
## Education



# 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 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.

The image shows a smartphone displaying the Splunk Answers website. The top navigation bar includes links to Splunk.com, Documentation, Splunkbase, Answers, Wiki, Blogs, and Developers. The user profile 'pwest\_splunk 20 • 1' is shown along with Logout and FAQ links. A search bar at the top right contains the placeholder 'Search Splunk Answers'. Below the header, there are two main call-to-action buttons: 'Find An Answer' (with a checkmark icon) and 'Find Splunk Apps' (with a gear icon). The 'Welcome to Splunk Answers' message encourages engagement with the Splunk community on Splunkbase. The 'Recent Answers' section lists three recent posts:

- Duo Connector App does not update index on dashboard when a different index is configured** (by Duo Splunk Connector, featured, commented 9 minutes ago by mmodestino [Splunk] 1k)
- Insufficient permissions with Free license** (by Website Input, commented 3 minutes ago by mmodestino [Splunk] 1k)
- Monitoring of Java Virtual Machines with JMX in Splunk** (by [redacted], commented 1 minute ago by [redacted] 1k)

On the right side of the phone screen, there is a promotional box for 'Splunk Enterprise Security' with the text 'Quickly detect and respond to internal and external attacks.' and a 'TRY IT NOW' button. Below the phone, a decorative graphic features diagonal stripes in white, pink, and orange.

# Developer Resources

<http://dev.splunk.com>

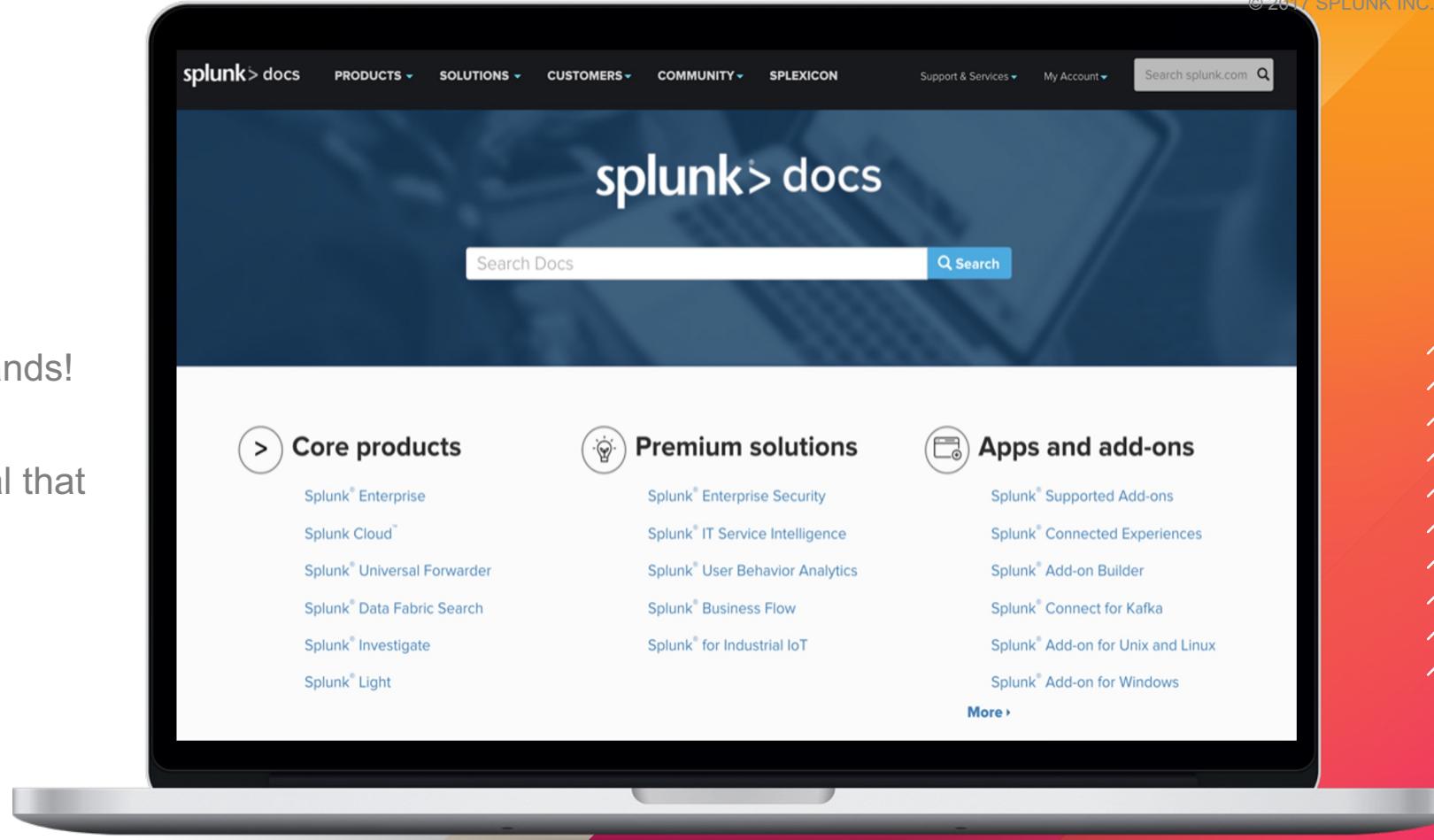
- > Check out our REST API and suite of SDKs to customise and extend the power of Splunk
- > Splunk integration with other applications and systems
- > Resources for building Splunk apps
- > Splunk Investigate

The tablet screen shows the "splunk>dev" website. The main heading is "Welcome to the Splunk Developer Program". Below it, a sub-headline reads "Build apps that Turn Data into Doing™ with Splunk." A "Learn more" button is present. To the right, a section titled "Featuring: Splunk Investigate" includes a brief description and a "Learn more >" link. Below this is a screenshot of the Splunk Investigate interface, showing a dashboard with various metrics and charts. At the bottom of the screen, there are two buttons: "Develop for Splunk Enterprise" and "Develop with Splunk Cloud Services", each with an arrow icon pointing to the right.

# Documentation

<https://docs.splunk.com>

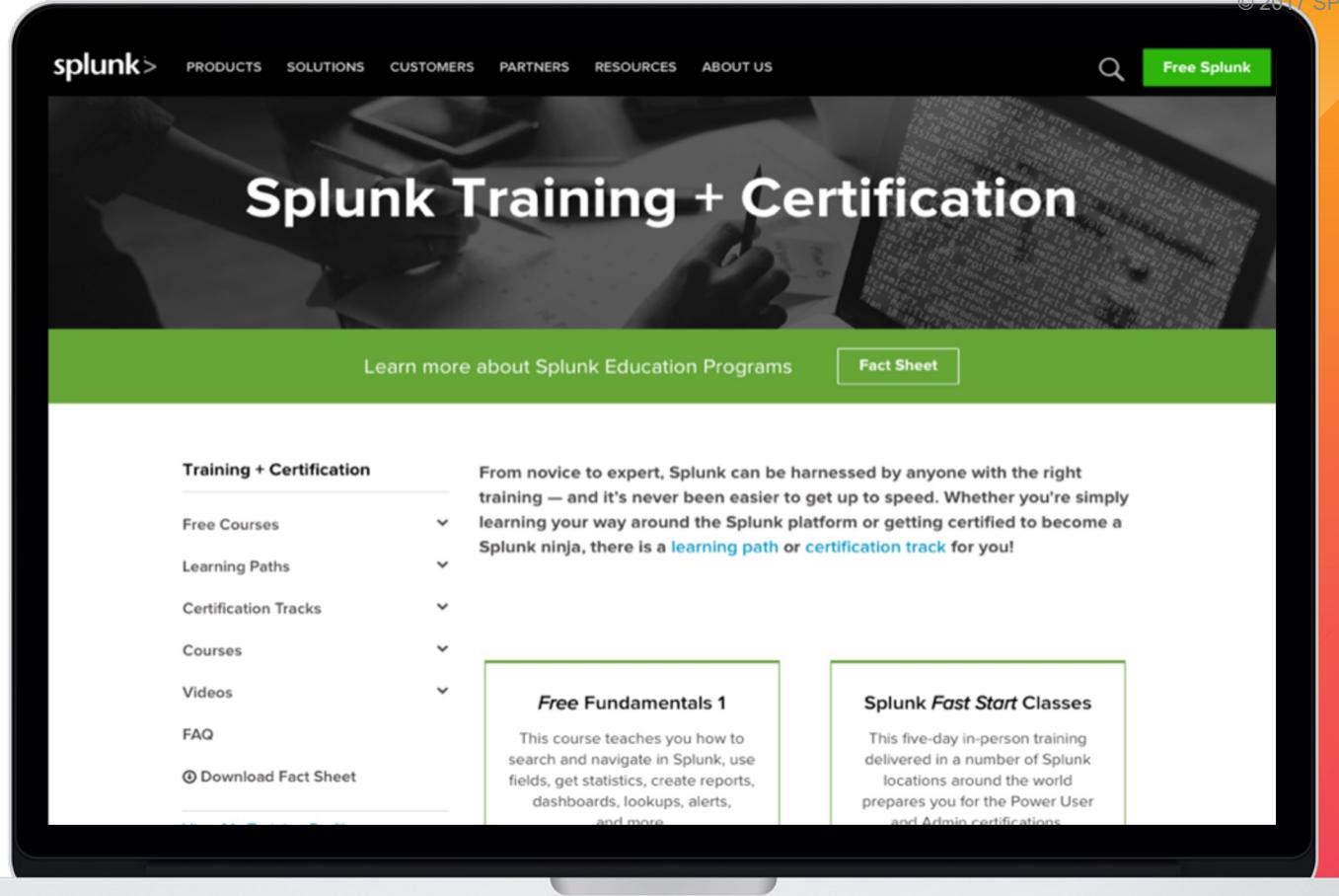
- > Splunk reference – Learn the commands!
- > Tutorials – Check out the search tutorial that even includes sample data to play with!
- > Use cases
- > References
- > Procedures/guides – installing, upgrading
- > And more!



# Education

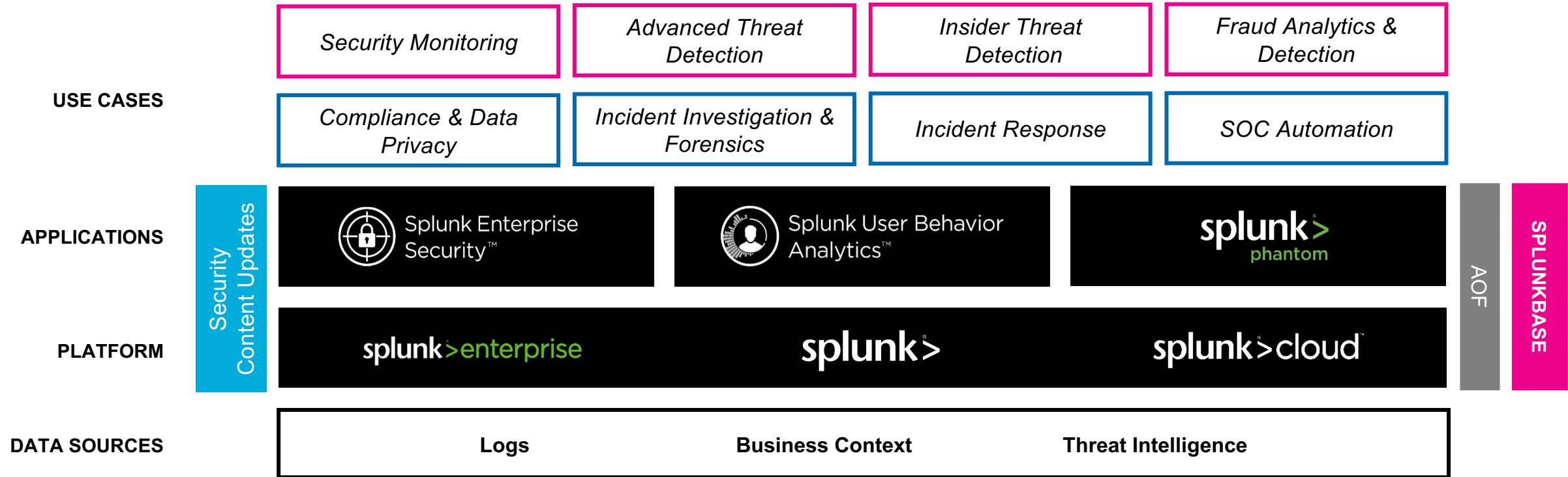
<https://www.splunk.com/education>

- > 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**



The image shows a smartphone displaying the Splunk Training + Certification page. The page has a dark background with a green header bar containing a search icon and a 'Free Splunk' button. The main title 'Splunk Training + Certification' is displayed prominently. Below the title is a green call-to-action button with the text 'Learn more about Splunk Education Programs' and a 'Fact Sheet' button. The left side of the screen features a sidebar with a section titled 'Training + Certification' and links to various resources: 'Free Courses', 'Learning Paths', 'Certification Tracks', 'Courses', 'Videos', and 'FAQ'. At the bottom of the sidebar is a link to 'Download Fact Sheet'. The right side of the screen contains descriptive text and two boxed sections: 'Free Fundamentals 1' and 'Splunk Fast Start Classes'.

# Security Operations Suite



# Thank You



**splunk**> turn data into doing™