

# Splunk Security 4 Rookies



#Splunk4Rookies

**splunk**<sup>®</sup> > turn data into doing<sup>™</sup>

# 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



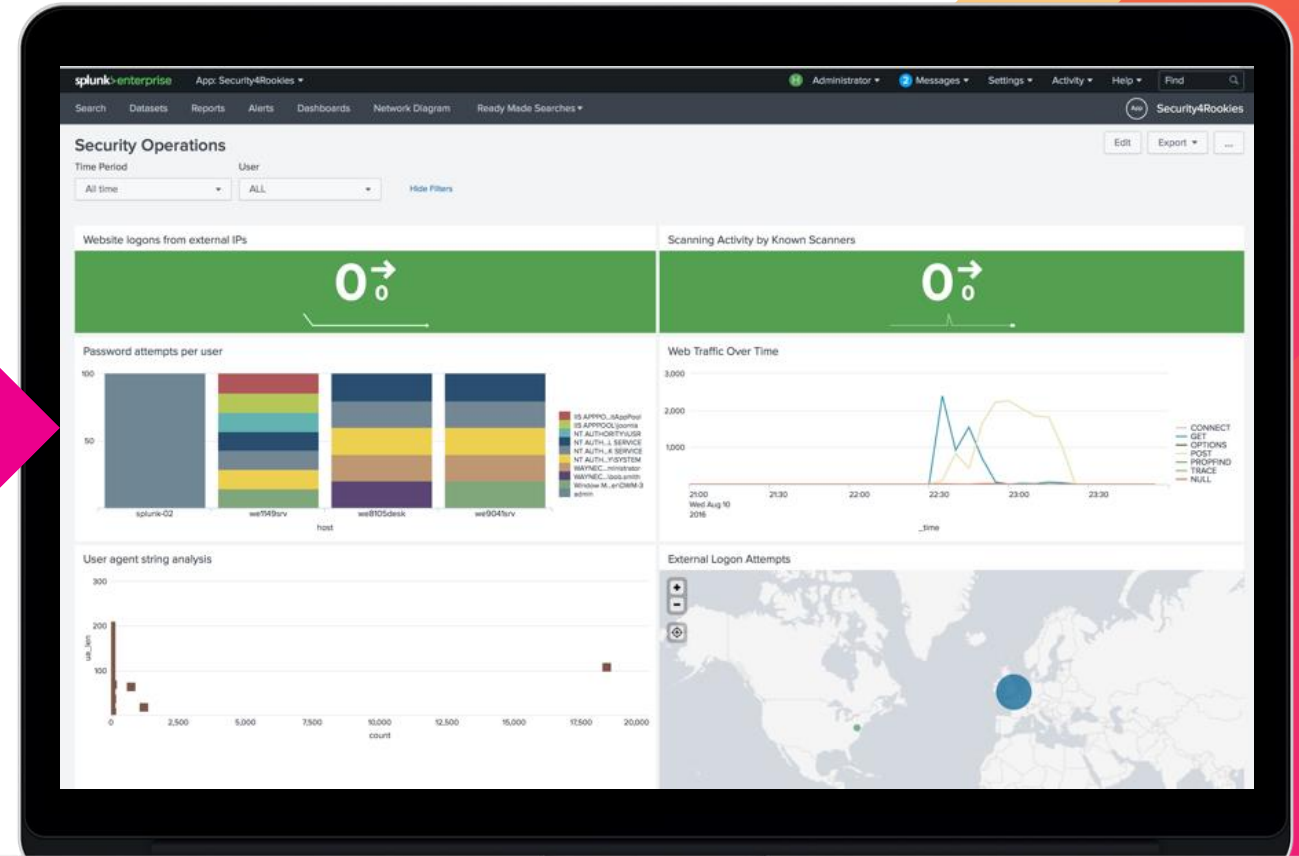
# There's a Lot More to Splunk...

- > 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 HTTP 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&JSESSIONID=SD3SL8FF4ADFF8 HTTP 1.1" 200 3350 "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 HTTP 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; en)" 389
125.17.14.100 - - [01/Nov/2016 20:48:26:174] "GET /product.screen?product_id=AV-CB-01&JSESSIONID=SD3SL10FF4ADFF2 HTTP 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=SD3SL1FF4ADFF3 HTTP 1.1" 200 2438 "http://www.myflowershop.com/cart.do?action=view&itemId=EST-18&product_id=FL-DLH-02" "Mozilla/5.0 (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=FL-DLH-02&JSESSIONID=SD3SL1FF4ADFF7 HTTP 1.1" 404 664 "http://www.myflowershop.com/product.screen?product_id=K9-BD-01" "Googlebot/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=SD4SL1FF4ADFF3 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&JSESSIONID=SD10SL9FF9ADFF7 HTTP 1.1" 200 933 "http://www.myflowershop.com/product.screen?product_id=AV-CB-01" "Googlebot/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 HTTP 1.1" 200 3491 "http://www.myflowershop.com/cart.do?action=addtocart&itemId=EST-6&product_id=AV-SB-02" "Googlebot/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; Intel 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; MSIE 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 HTTP 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:

[http://splunk4rookies.com/<session#>/self\\_register](http://splunk4rookies.com/<session#>/self_register)

### 2. Download today's slide deck:

<http://bit.ly/Security-S4R-Attendee>

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://ec2-34-252-66-91.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

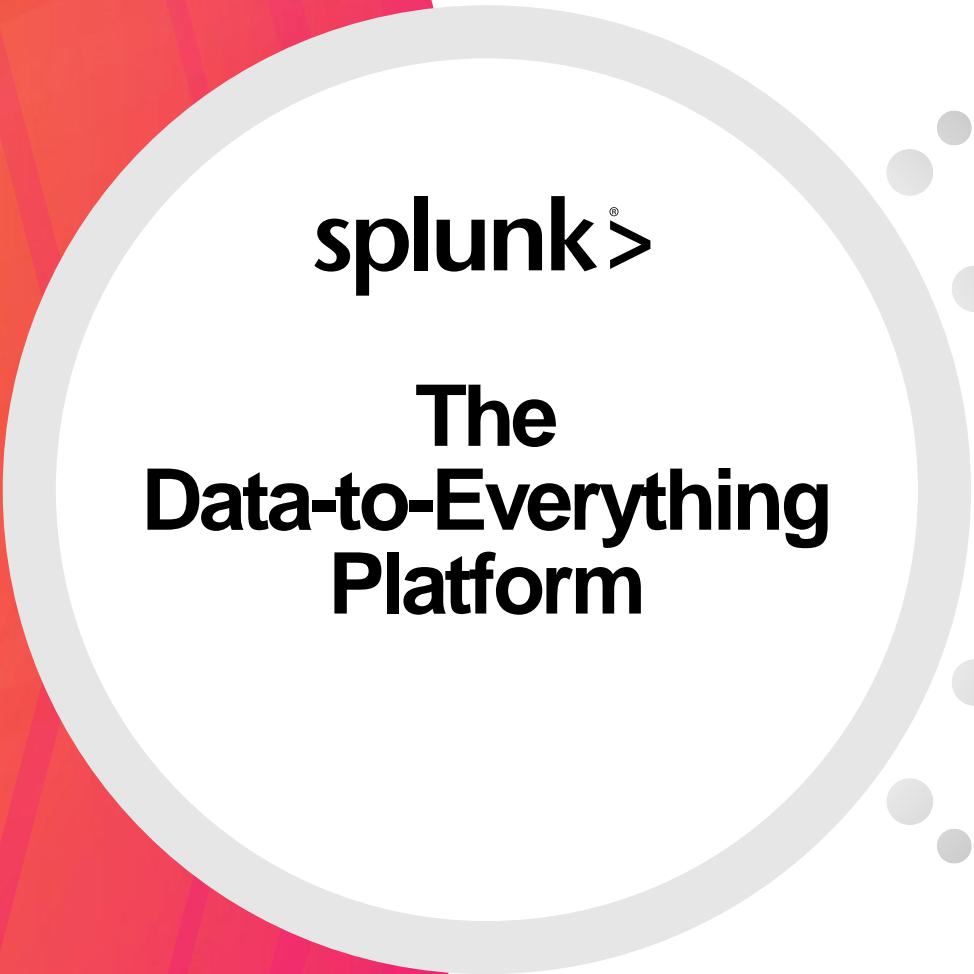





# Turning Real-time Data Into Action is Hard







# splunk>

## The Data-to-Everything Platform



**IT**



**Security**



**AppDev**



**Biz  
Analytics**

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

ANALYZE

ACT

INVESTIGATE

MONITOR



**IT**



**Security**



**AppDev**



**Biz Analytics**

# Our Investigative Approach

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

## Send

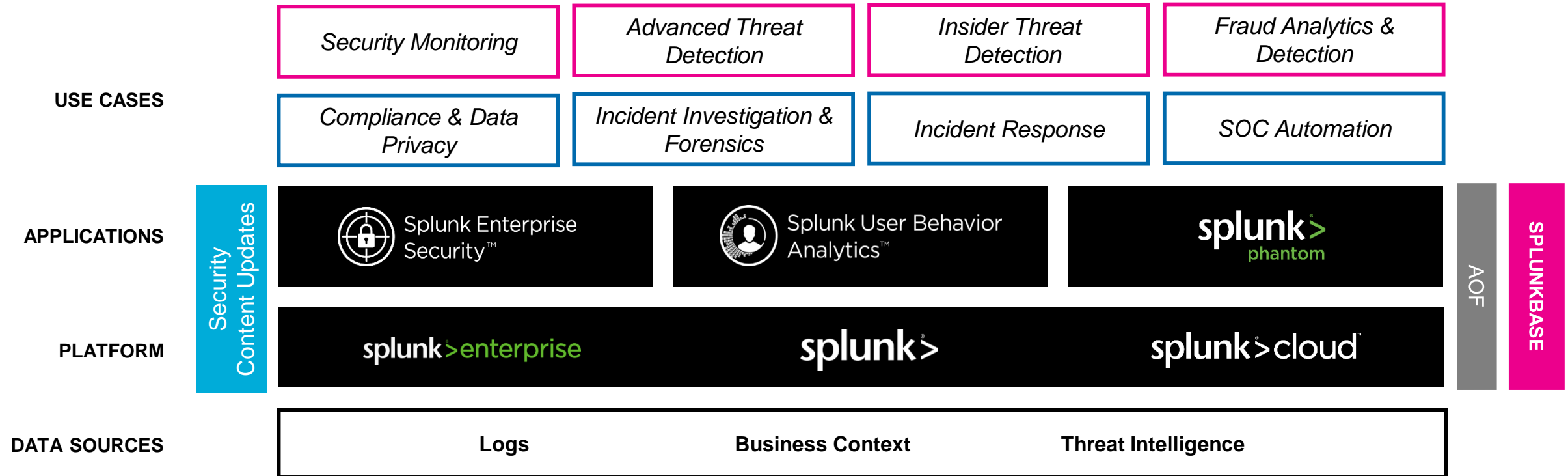
unstructured data from all  
systems, devices, and people

## React

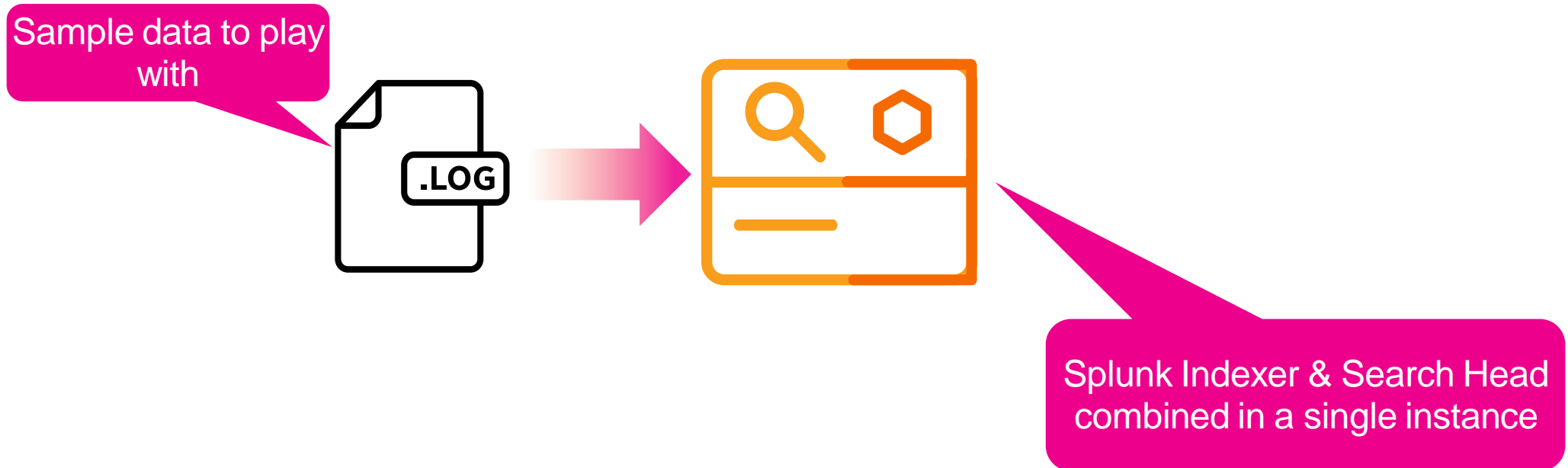
quickly to changing circumstances by  
asking questions immediately

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

# Security Operations Suite



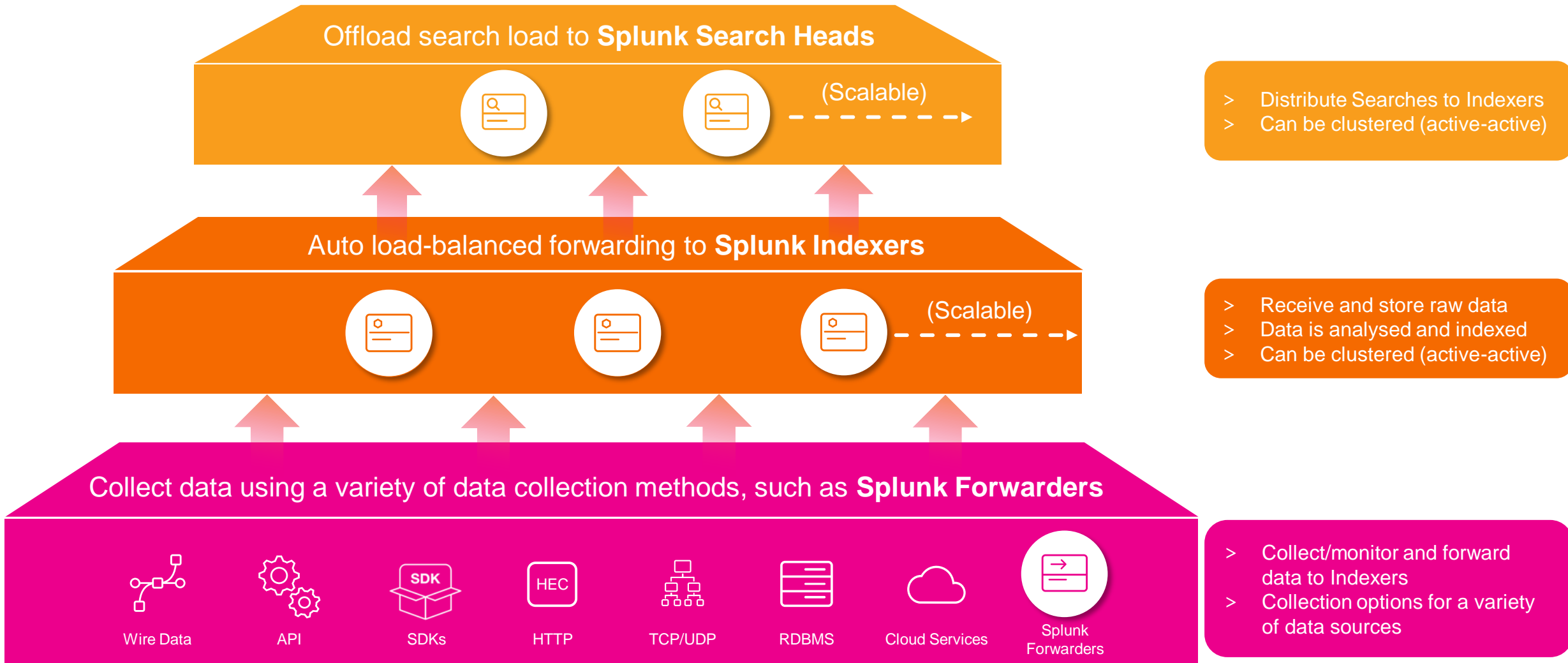
# Today's Environment





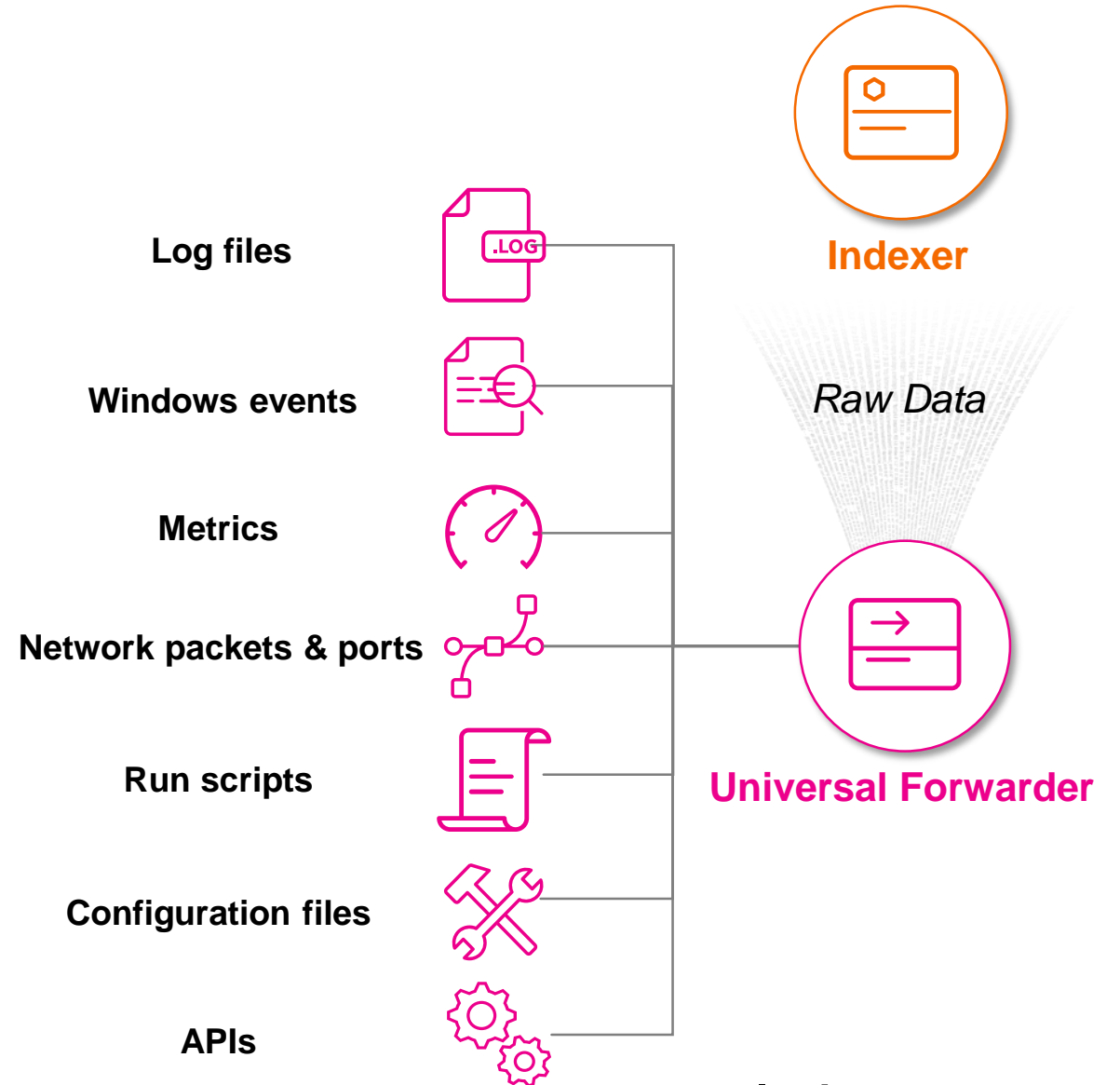
# Scales to Petabytes Per Day

Enterprise-Class Scale, Resilience and Interoperability



# What is a Universal Forwarder?

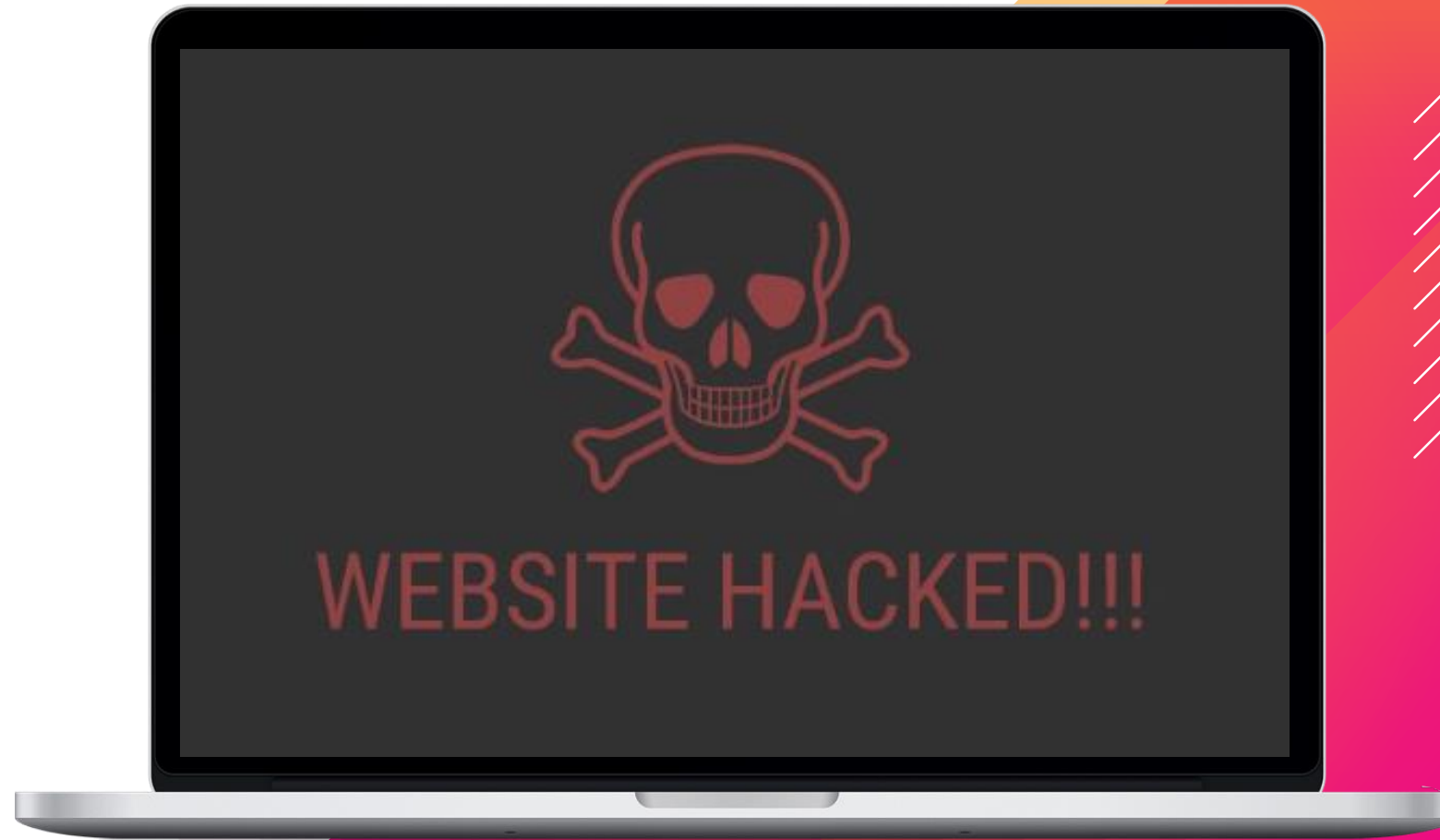
- > Reliable collection of data from remote locations
- > Includes methods for collecting from a variety of data sources
- > Simple, but packed with lots of goodness:
  - ✓ Buffering / guaranteed delivery
  - ✓ Encryption
  - ✓ Compression
  - ✓ Load balancing
  - ✓ And more!
- > Very small footprint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



imreallynotbatman.com

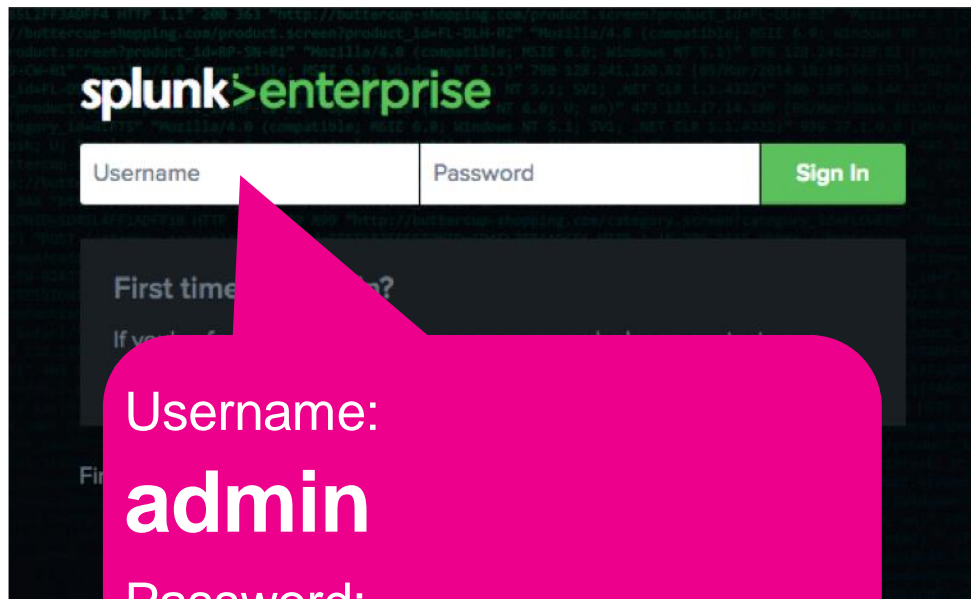
# Security Data and Searches

For Security People



# Let's Go!

# Log in to Splunk

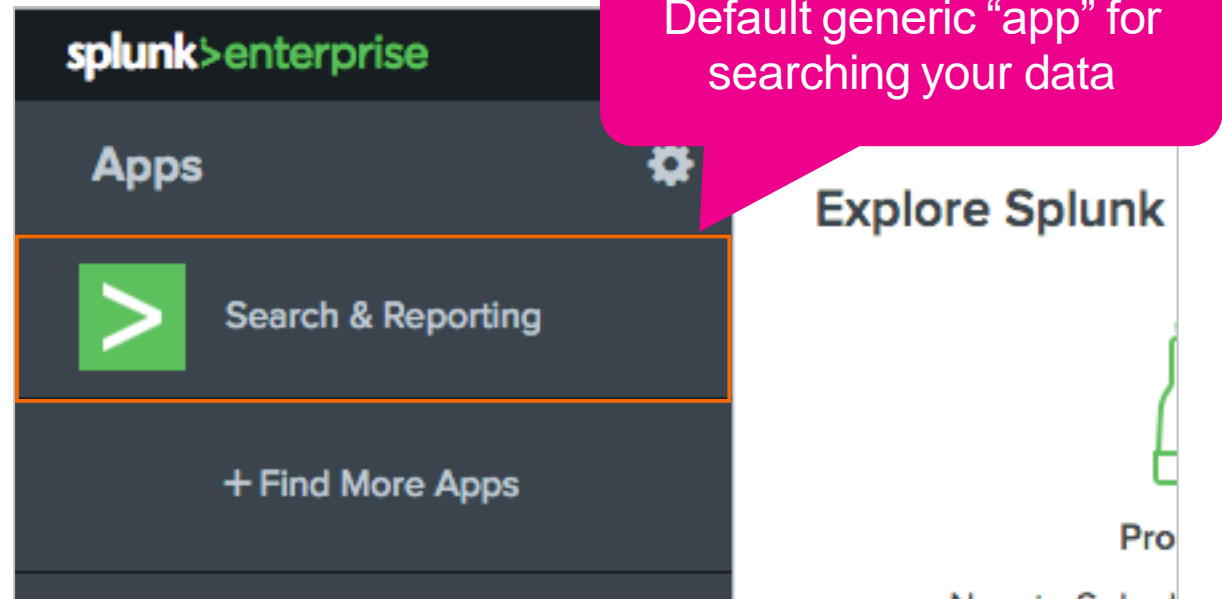


Username:

**admin**

Password:

**security4rookies**



Default generic “app” for searching your data



# 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!



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

< Back **3**

Chpt1 - Search 1

Chpt1 - Search 2

Chpt1 - Search 3

Chpt1 - Search 4

Chpt1 - Search 5

Click Here!

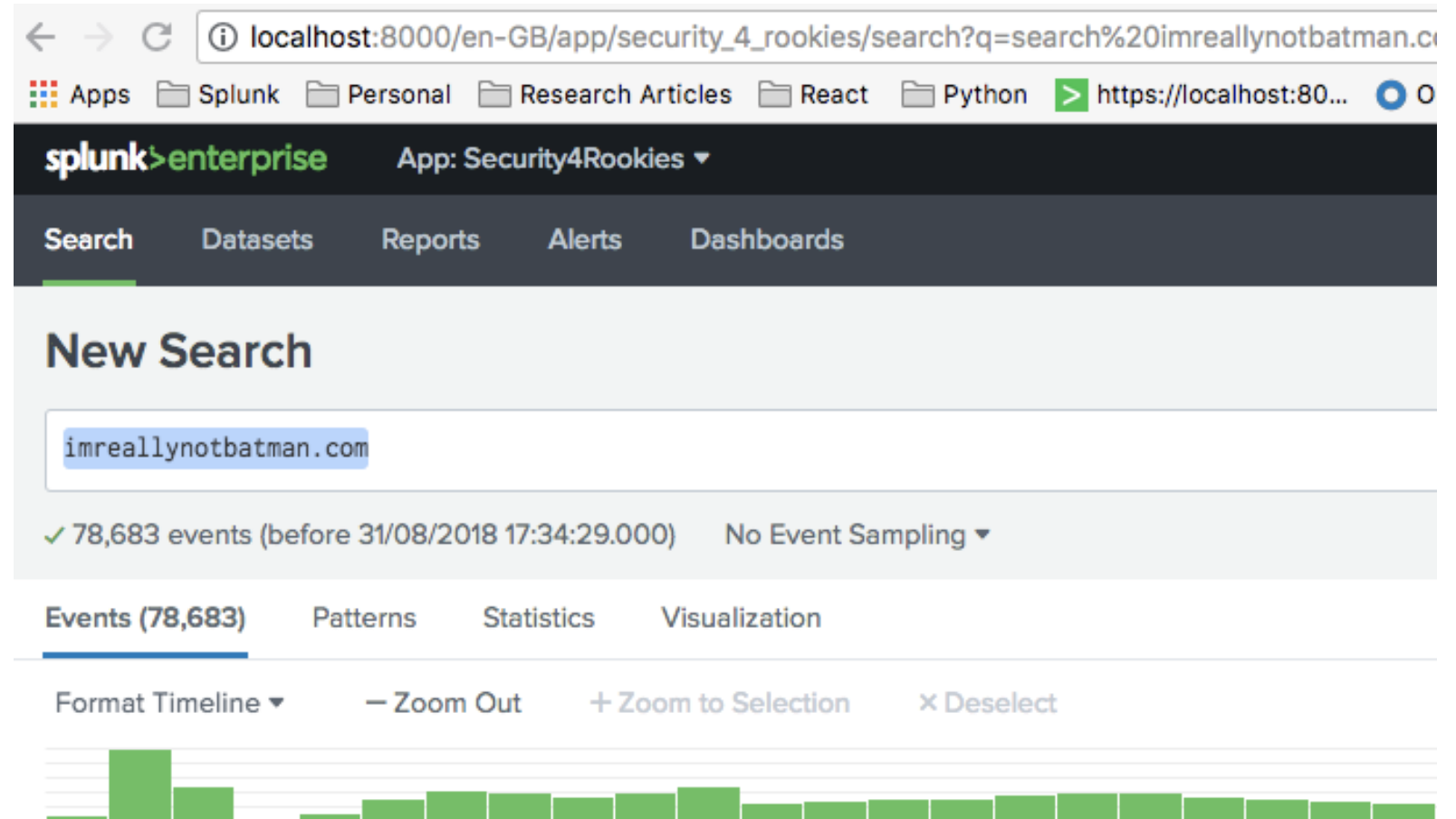
# Search Basics

## Chpt1 – Search 1

### Literal Strings

### Manual

imrealllynotbatman.com



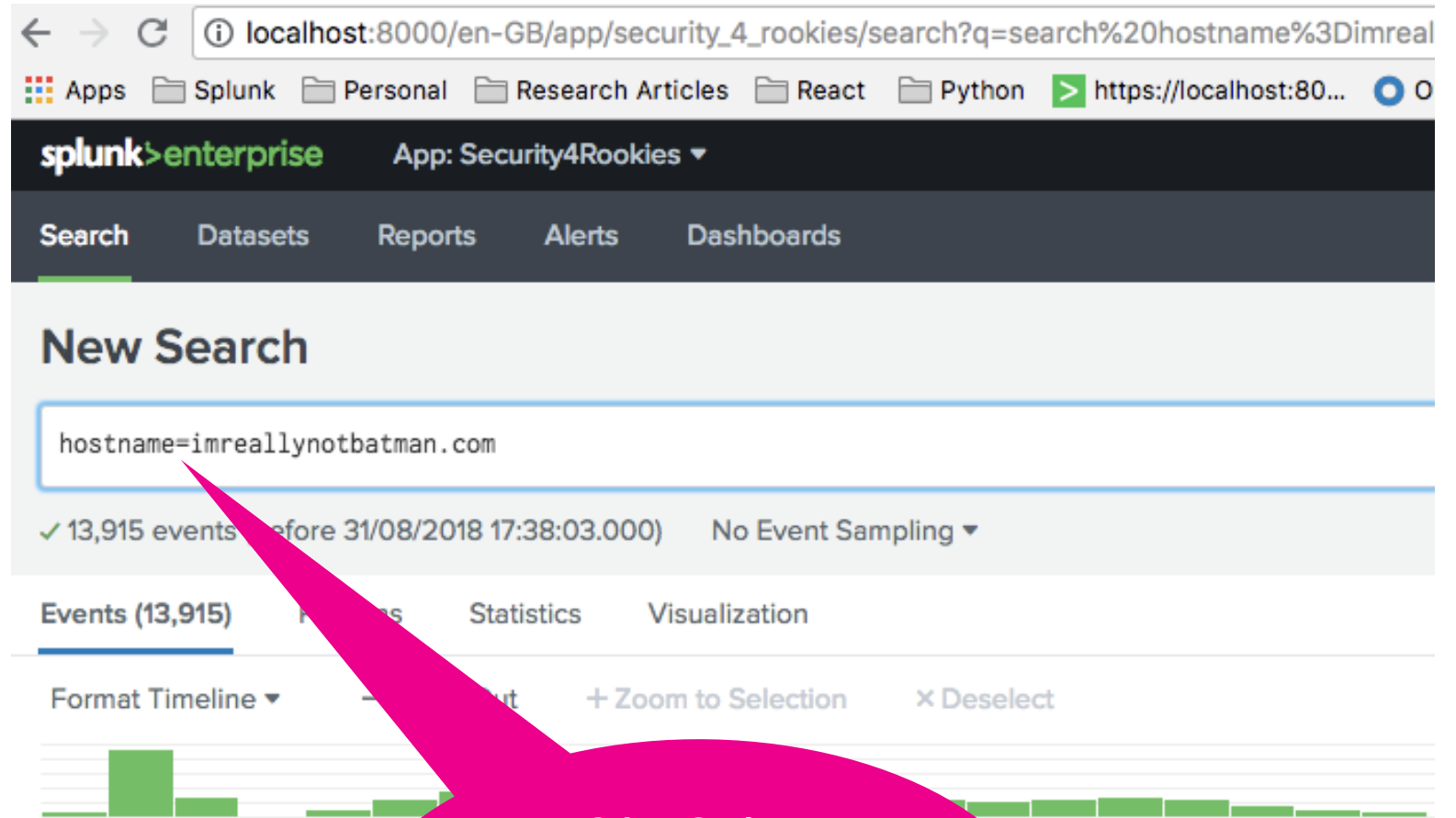
# Search Basics

## Chpt1 – Search 2

Key=Value pair searching

### Manual

hostname="imreallynotbatman.com"



#### Other Options

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



# Search Basics

## Chpt1 – Search 3

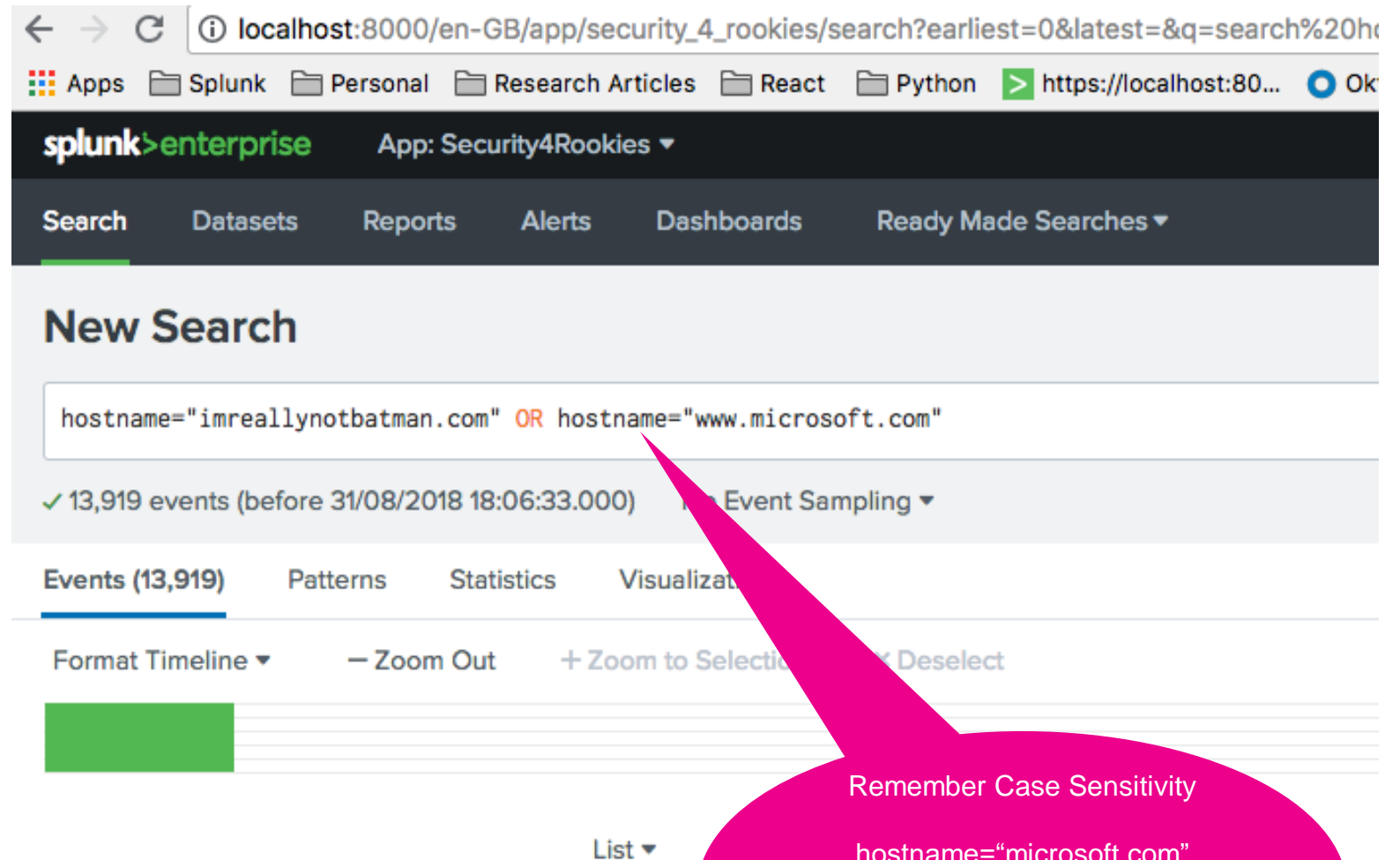
### Using OR

### Manual

hostname="imreallynotbatman.com"

OR

hostname="www.microsoft.com"



Remember Case Sensitivity

hostname="microsoft.com"

**NOT** the same as

HOSTNAME="microsoft.com"

# Search Basics

## Chpt1 – Search 4

### Using Wildcards

## Manual

\*3791

The screenshot shows the Splunk Enterprise web interface. The browser address bar displays the URL: `localhost:8000/en-GB/app/security_4_rookies/search?s=%2FservicesNS%2Fnobody%2F...`. The Splunk logo and "enterprise" text are visible in the top left. The application name "App: Security4Rookies" is shown in the top right. The navigation bar includes links for Search, Datasets, Reports, Alerts, Dashboards, and Ready Made Searches. The main heading is "Chpt1 - Search 4". A search input field contains the query `*3791`. Below the search bar, it indicates "35 of 304,517 events matched" and "No Event Sampling". The "Events (35)" tab is selected, showing a list of events. The first event is visible, dated "24 Aug 2016 17:53".

# Search Basics

## Chpt1 – Search 5

### Using Wildcards

#### Manual

3791\*exe

The screenshot shows the Splunk Search interface in a web browser. The address bar displays the URL: `localhost:8000/en-GB/app/security_4_rookies/search?q=search%203791*exe&display.pag`. The browser's tab bar shows several tabs: 'Apps', 'Splunk', 'Personal', 'Research Articles', 'React', 'Python', and a new tab for 'https://localhost:80...'. The Splunk header shows 'splunk>enterprise' and 'App: Security4Rookies'. The navigation bar includes 'Search', 'Datasets', 'Reports', 'Alerts', 'Dashboards', and 'Ready Made Searches'. The main section is titled 'New Search' and contains a search bar with the query '3791\*exe'. Below the search bar, it indicates '✓ 11 events (before 31/08/2018 18:44:01.000)' and 'No Event Sampling'. The interface has tabs for 'Events (11)', 'Patterns', 'Statistics', and 'Visualization'. The 'Events (11)' tab is active, showing a timeline view with three green bars representing events. Above the timeline are controls: 'Format Timeline', 'Zoom Out', 'Zoom to Selection', and 'Deselect'. Below the timeline are options 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

a host 1  
a source 4  
a sourcetype 1

#### INTERESTING FIELDS

a control 1  
# count 9  
a 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
```

# Search Basics

## Chpt1 – Search 6

### CIDR Matching

### Manual

dest\_ip=192.168.250.0/24

```
# bytes_in 100+
# bytes_out 100+
a command{} 20
# date_hour 9
# date_mday 2
# date_minute 60
a date_month 1
# date_year 2018
a dest_ip 192.168.250.0/24
# dest_ip 192.168.250.0/24
a dv 1
a endtime 2018-08-24T10:27:43.273000Z
a index 1
# linecount 1
a nt_status{} 25
# packets_in 100+
# packets_out 100+
a punct 100+
```



\_DSS\_WITH\_AES\_256\_CBC\_SHA256", "TLS\_DH\_anon\_WITH\_AES\_256\_GCM\_SHA384", "TLS\_DH\_anon\_W

**dest\_ip** ×

7 Values, 100% of events Selected Yes No

**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%

7 [ endtime : 2018-08-24T10:27:43.273000Z ; timestamp : 2018-08-24T10:27:43.273000Z ]

# 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

i	Time	Event
>	24/08/2016 18:19:15.000	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><Syst 5698FFB09' /><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='Destinatio = 'DestinationHostname'></Data><Data Name='DestinationPort'>64108</Data><De 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 5698FFB09' /><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='Destinatio = 'DestinationHostname'></Data><Data Name='DestinationPort'>64062</Data><De

| 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>

# 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.
```

WinEventLog:Security

Multi Line Breaking  
Complex Field Extractions  
Process ID needs Hex Decoding

#### 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
```

```
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

The left screenshot shows the Splunk Enterprise search interface. The search bar contains the query `index=botsv1 sourcetype=fgt_utm`. The results show 25,586 events. A pink arrow labeled '1' points to the 'Event' column. A pink arrow labeled '2' points to the 'Event Actions' dropdown menu.

The right screenshot shows the 'Event Actions' menu open. A pink arrow labeled '3' points to the 'Extract Fields' option. Below the menu, a table shows the extracted fields and their values.

Field	Value
host	192.1
source	udp
sourcetype	fgt_utm
action	allow
app	NTP
appcat	Netw
appid	1627



# Field Extraction Basics

## Chpt2 – Search 1

### Extract the field

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

splunk enterprise App: Security4Rookies Administrator Messages Settings Activity Help

Extract Fields Select Method Select Fields Save Next >

### Select Method

Indicate the method you want to use to extract your field(s). [Learn more](#)  
[I prefer to write the regular expression myself](#)

Source type **fgt\_utm**

```
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
```

#### Regular Expression

**(.\*?)**

Splunk Enterprise will extract fields using a Regular Expression.

#### Delimiters

**x|y|z**

Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).

# Field Extraction Basics

Chpt2 – Search 1

Highlight and Name

localhost:8000/en-GB/app/security\_4\_rookies/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

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an ever already 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=1055  
srcip=192.168.250.1 dstip=91.189.91.157 dstport=123 proto=17 service="NTP" policyid=  
msg=

Extract Require

Field Name src\_ip

Sample Value 192.168.250.1

Add Extraction

1. Highlight field

2

3

# Field Extraction Basics

## Chpt2 – Search 1

## Verify Fields and Set Access Rights

The screenshot displays the Splunk Field Extraction wizard interface. The progress bar at the top indicates the current step in the process: Select Method, Select Fields, Validate, and Save.

**Step 1: Select Fields** (labeled with a pink arrow and the number 1). The "Select Fields" section shows a sample event with various fields. The "Preview" section shows the selected fields and a filter. The "Values" section lists the extracted values.

**Step 2: Verify Values** (labeled with a pink arrow and the number 2). The "Verify Values" section shows the selected fields and a filter. The "Values" section lists the extracted values.

**Step 3: Save** (labeled with a pink arrow and the number 3). The "Save" section shows the extraction name, owner, app, and permissions. The "Permissions" table shows the read and write permissions for different roles.

**Step 4: Finish** (labeled with a pink arrow and the number 4). The "Finish" button is highlighted, indicating the end of the process.

**Extractions Name:** EXTRACT- src\_ip

**Owner:** admin

**App:** security\_4\_rookies

**Permissions:**

	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>

**Source type:** fgt\_utm

**Sample event:** Aug 24 12:27:14 192.168.250.1 date=2016-08-24 time=12:27:14 devname=gotham-fortigate devid=FGT604614044725 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 dstport=123 proto=17 service=NTP policyid=10 sessionid=4237590 applist=HoneyPot-Access appcat=Network.Service app=NTP action=pass msg=Network.Service: NTP, aprisk=elevated

**Fields:** src\_ip

**Regular Expression:** ^(?!(^ \n)\* )\$[?P<src\_ip>(^ )\$]

# 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

Eventtype

Tag

Tag

Windows Logon Success Event

} win\_auth\_success

Linux Logon Success Event

} nix\_auth\_success

VPN Logon Success Event

} vpn\_auth\_success

success

Windows Logon Failure Event

} win\_auth\_failure

Linux Logon Failure Event

} linux\_auth\_failure

VPN Logon Failure Event

} vpn\_auth\_failure

failure

authentication



# 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"%20

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

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

< Hide Fields		≡ All Fields		i	Time	Event
SELECTED FIELDS				>	24/08/2016 19:27:24.000	08/24/2016 11:27:24 AM LogName=Security SourceName=Microsoft Windows security
a host 3						

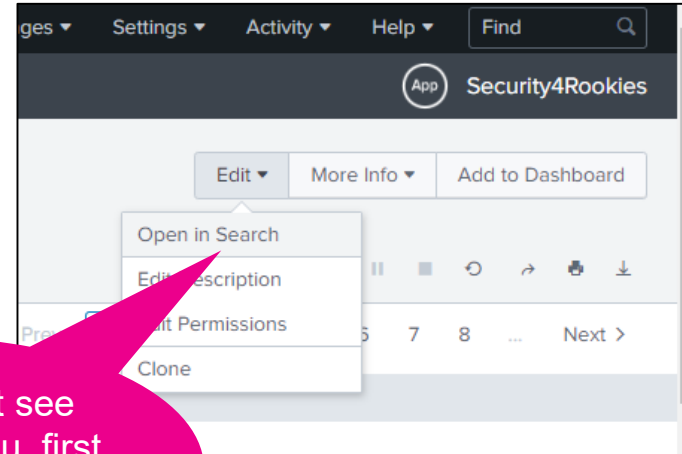
# Event Types & Tags Basics

## Chpt3 – Search 1

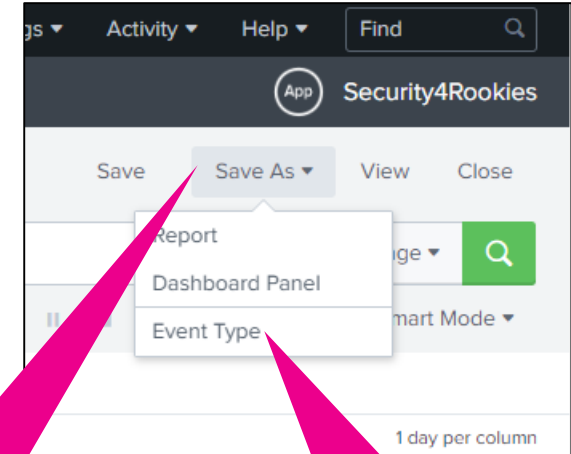
### Creating an Eventtype

#### 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"

A screenshot of the 'Save As Event Type' dialog box in Splunk. It contains the following fields:

- Name: win\_auth\_success
- Tags: success, authentication
- Color: none
- Priority: 1 (Highest)

At the bottom are 'Cancel' and 'Save' buttons. A pink callout bubble points to the 'Save' button.

4. Enter Event Type name "win\_auth\_success"

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

6. "Save"

# Event Types & Tags Basics

## Chpt3 – Search 2

### Searching by tags

## Manual

tag=authentication tag=success

**1. Click “eventtype”**

**2. Note that our new Event Type is shown**

**eventtype**

1 Value, 100% of events

Selected ☒ Yes ☐ No

**Reports**

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

Events with this field

Values	Count	%
<a href="#">win_auth_success</a>	3,209	100%

EventCode=4624  
EventTtype=0

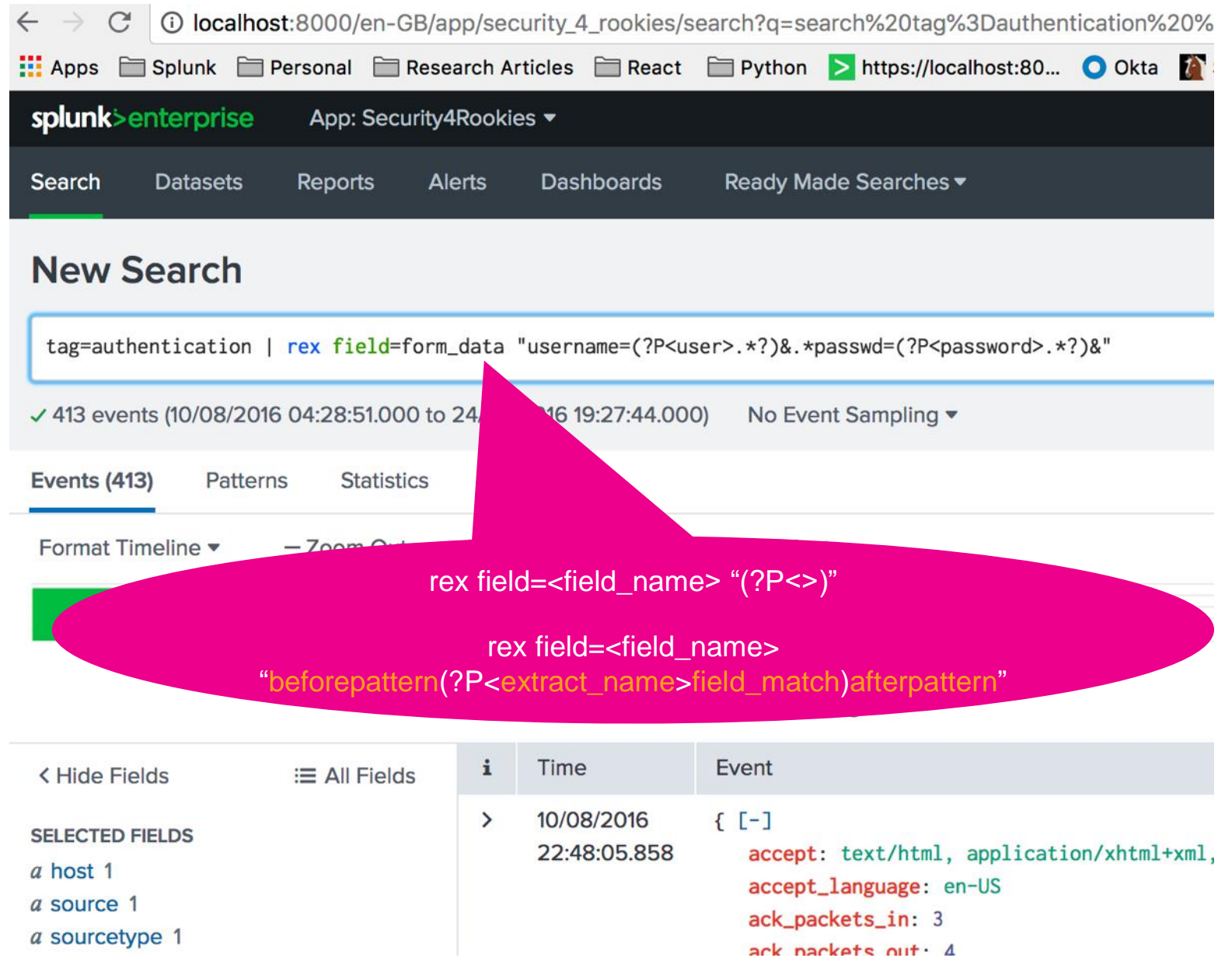
# Bonus Material

## Chpt3 – Search 3

### REGEX for the brave

#### Manual

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



The screenshot shows the Splunk Enterprise web interface at localhost:8000. The search bar contains the query: `tag=authentication | rex field=form_data "username=(?P<user>.*?)&.*passwd=(?P<password>.*?)&"`. The search results show 413 events. A pink callout bubble highlights the regex syntax:

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

The results table shows the following data:

< Hide Fields	≡ All Fields	i	Time	Event
SELECTED FIELDS		>	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



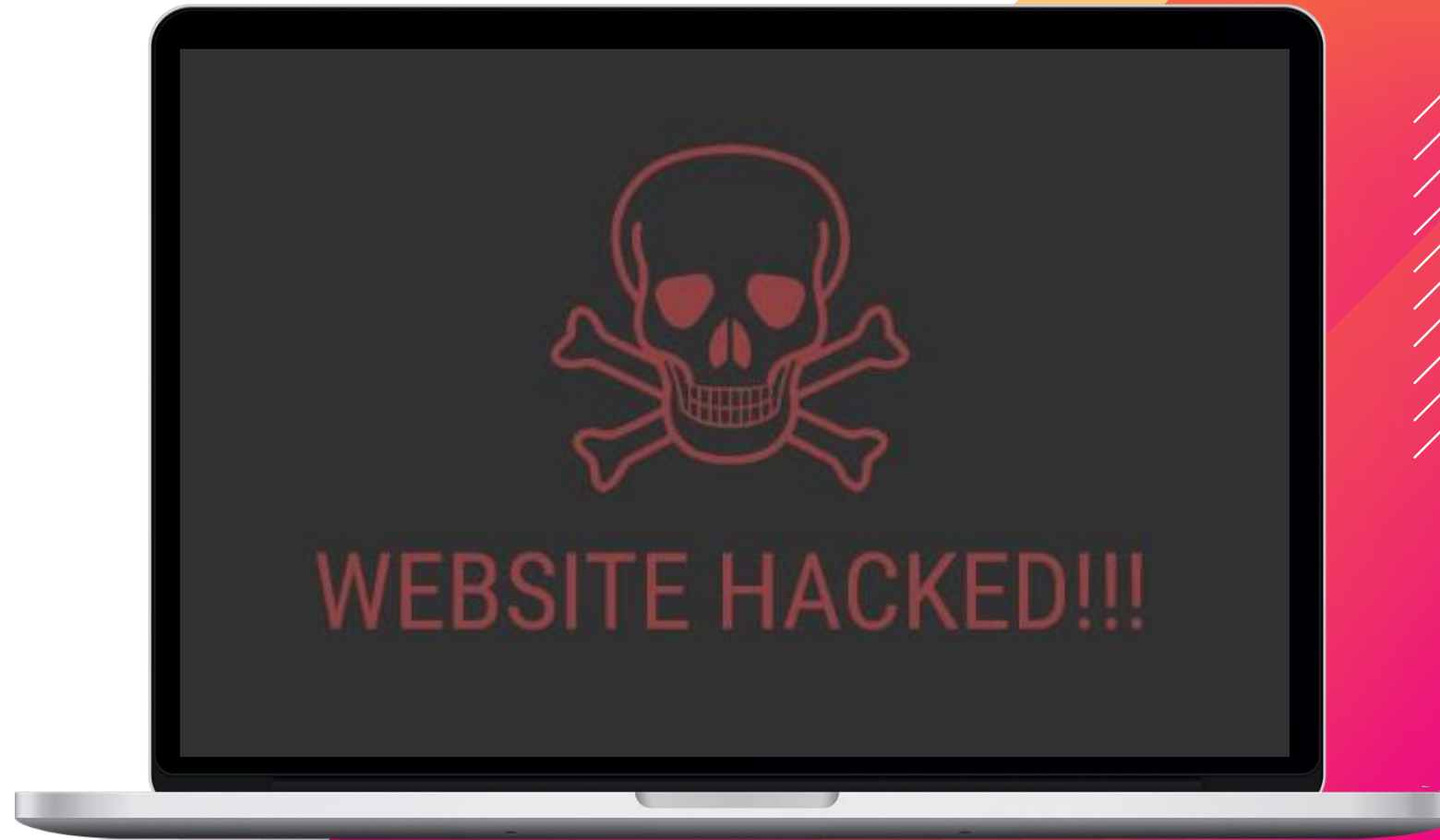
# Plugging it all together

Where the rubber meets the road

imrealllynotbatman.com

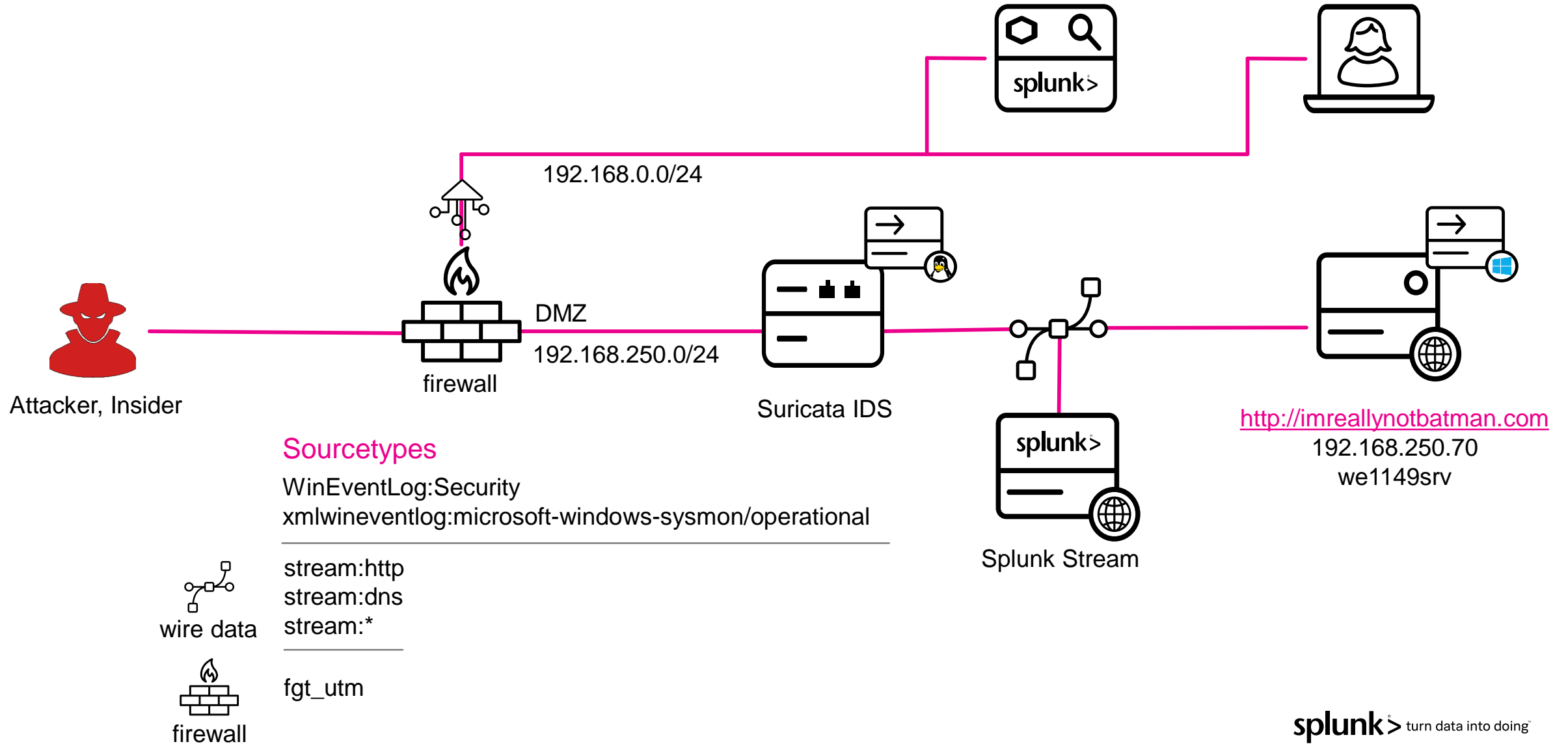
# Security Data and Searches

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 web interface in a browser. The address bar displays `localhost:8000/en-GB/app/security_4_rookies/search?q=search%20index%3D%22botsv1%22%20sourcetype%3Dstream%3Ahttp%20dest_ip%3D192.168.250.70`. The top navigation bar includes links for Apps, Splunk, Personal, Research Articles, React, and Python. The main header shows the Splunk logo and the app name "Security4Rookies". Below the header is a navigation menu with "Search" (highlighted), "Datasets", "Reports", "Alerts", "Dashboards", and "Ready Made Search". The "New Search" section contains a search bar with the query `index="botsv1" sourcetype=stream:http dest_ip=192.168.250.70`. Below the search bar, a status bar indicates "✓ 20,275 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000) No Event Sa". The "Events (20,275)" tab is selected, showing a timeline visualization with a green bar representing the event data. Other tabs include "Patterns", "Statistics", and "Visualization". At the bottom of the timeline, there are controls for "Format Timeline", "Zoom Out", "Zoom to Selection", and "Deselect".

# 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 Search interface for the 'Security4Rookies' app. The search bar contains the query: `index="botsv1" sourcetype=stream:http dest_ip=192.168.250.70 | stats count(src_ip) BY src_ip`. Below the search bar, it indicates 20,275 events. The 'Statistics (3)' tab is selected, showing a table of results. A pink callout points to the search bar with the text 'Filter Statements'. Another pink callout points to the 'stats count(src\_ip) BY src\_ip' part of the query with the text 'Aggregate & count'.

src_ip
192.168.250.70
23.22.63.114
40.80.148.42

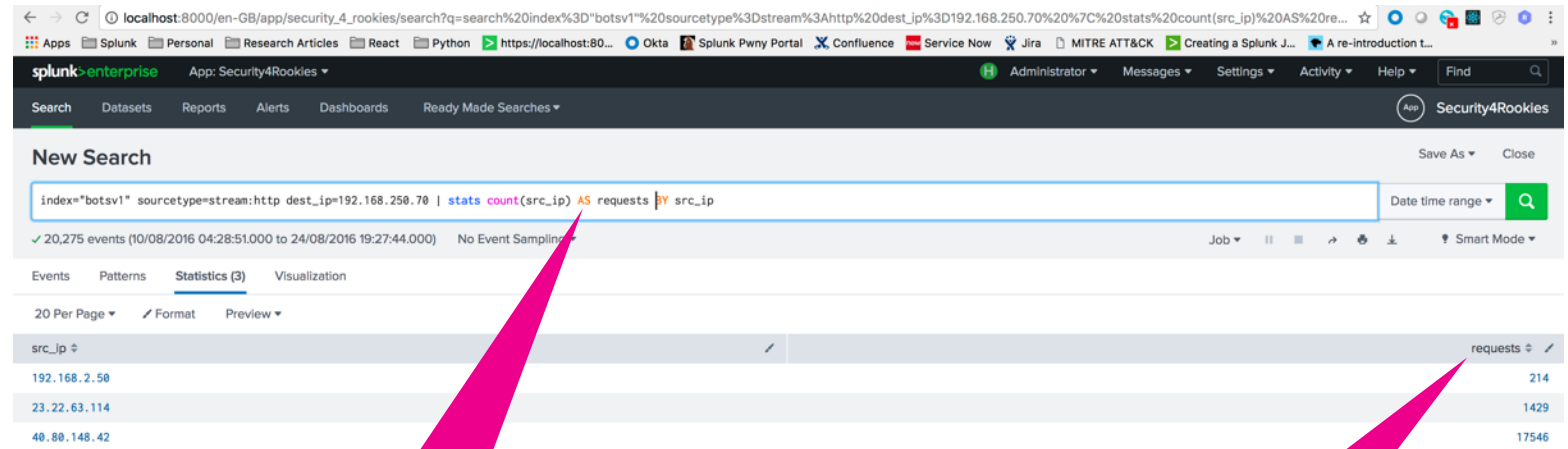
# Discovering the attack

## 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
```



The screenshot shows the Splunk Search interface with a search bar containing the query: `index="botsv1" sourcetype=stream:http dest_ip=192.168.250.70 | stats count(src_ip) AS requests BY src_ip`. The search results are displayed in a table with the following data:

src_ip	requests
192.168.2.50	214
23.22.63.114	1429
40.80.148.42	17546

AS clause renames

New field name

# 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
```

Optional minus = descending order

Sorted Order

src_ip	requests
40.80.148.42	17546
23.22.63.114	1429
	214



# Discovering the attack

## Chpt4 – Search 5

## Investigating the source headers

### Manual

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

**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 Ev

Events (20,275) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

Hide Fields All Fields

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
- # c\_ip 93
- a splunk\_server
- a src\_content 100+
- a src\_headers 100+
- a src\_ip
- a src\_mac
- src\_port 100+

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 Accept-Encoding: identity Host: imreallynotbatman.com Connection: close User-Agent: Python-urllib/2.7	412	2.147%
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-xbitmap, image/jpeg, image/pjpeg, image/png, */*	88	0.458%
POST /joomla/index.php/component/search/ HTTP/1.1 Content-Length: 121 Content-Type: application/x-www-form-urlencoded Referer: http://imreallynotbatman.com:80/ Cookie: ae72c62a4936b238523950a4f26f67d0=v7ikb3iet3vphv3 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: */*	88	0.458%

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 Alerts Dashboards Network Diagram Ready Made Searches Downloads App Security4Rookies

### Chpt4 - Search 6

Save Save As View Close

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 Date time range

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

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
```

splunk>enterprise App: Security4Rookies 2 Messages Settings Activity Help Find

Search Datasets Reports Alerts Dashboards Network Diagram Ready Made Searches Downloads App Security4Rookies

### Chpt4 - Search 7

Save Save As View Close

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 Date time range

✓ 12,844 events (10/08/2016 03:28:51.000 to 24/08/2016 18:27:44.000) No Event Sampling Job 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	count
&ordering=!()'&!* &searchphrase=all&searchword=&task=search	1
&ordering=!()'&!* &searchphrase=all&searchword=e&task=search	1
&ordering=!()'&!* &searchphrase=all&searchword=the&task=search	1
&ordering=!()'&!* &searchphrase=any&searchword=&task=search	1
&ordering=!()'&!* &searchphrase=exact&searchword=&task=search	1
&ordering=!()'&!* &searchphrase=exact&searchword=the&task=search	1
&ordering="+response.write(9006556*9070592)+"&searchphrase=all&searchword=&task=search	1
&ordering="+response.write(9141042*9254568)+"&searchphrase=exact&searchword=the&task=search	1
&ordering="+response.write(9248686*9127579)+"&searchphrase=any&searchword=the&task=search	1
&ordering="+response.write(9372747*9029690)+"&searchphrase=any&searchword=&task=search	1
&ordering="+response.write(9450103*9133714)+"&searchphrase=exact&searchword=&task=search	1
&ordering="+response.write(9508155*9173884)+"&searchphrase=all&searchword=e&task=search	1
&ordering="+response.write(9627406*9035038)+"&searchphrase=all&searchword=the&task=search	1
&ordering=";print(md5(acunetix_wvs_security_test));\$a="&searchphrase=all&searchword=e&task=search	1
&ordering=";print(md5(acunetix_wvs_security_test));\$a="&searchphrase=all&searchword=the&task=search	1

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

# Discovering the attack

## Chpt4 – Search 8

### Investigating login activity

#### Manual

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

**New Search**

index="botsv1" sourcetype=stream:http http\_method="POST" form\_data=\*username\*passwd\*

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

Events (413) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection

Hide Fields All Fields

form\_data

>100 Values, 100% of events

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values

Value	Count	%
username=admin&0960d493674eb04861bd64da9b662118=1 &task=login&return=aW5kZXgucGhw&option=com_login&passwd=arthur	1	0.242%
username=admin&0eda02d7478dfb4164170ef384807a=1 &task=login&return=aW5kZXgucGhw&option=com_login&passwd=bigdaddy	1	0.242%
username=admin&115c3aa6072f4b02b4354909431510f6=1 &task=login&return=aW5kZXgucGhw&option=com_login&passwd=blazer	1	0.242%
username=admin&12c709bcc2e14d5a015f054d18d36537=1 &task=login&return=aW5kZXgucGhw&option=com_login&passwd=fire	1	0.242%
username=admin&2a2ddf97716c1d1e9da21cdf82b231e=1 &task=login&return=aW5kZXgucGhw&option=com_login&passwd=777777	1	0.242%
username=admin&2c340c4e46444ba249ff7e599e6dfa52=1 &task=login&return=aW5kZXgucGhw&option=com_login&passwd=flower	1	0.242%
username=admin&32c15329bc3f78039869bb3bf17c28a6=1 &task=login&return=aW5kZXgucGhw&option=com_login&	1	0.242%

# 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"
```

```
# date_zone 1
a dest_content 1
a dest_headers 1
a dest_ip 1
a dest_mac 1
# dest_port 1
# duplicate_packets_in 1
# duplicate_packets_out 1
a endtime 1
a eventtype 1
a form_data 1
a http_comment 1
# http_content_length 1
a http_content_type 1
a http_method 1
a http_referrer 1
a http_user_agent 1
a index 1
# linecount 1
a location 1
# missing_packets_in 1
# missing_packets_out 1
a network_interface 1
```

```
dest_ip: 192.168.250.70
dest_mac: 00:0C:29:C4:02:7E
dest_port: 80
duplicate_packets_in: 1
```

#### form\_data

1 Value, 100% of events

Selected

Yes

No

#### Reports

Top values

Top values by time

Rare values

Events with this field

#### Values

Count

%

Values	Count	%
username=admin&passwd=batman&option=com_login&task=login&return=aW5kZXgucGhw&5ec827a3f67ce0efc546d81f7356acc=1	1	100%

```
packets_out: 5
reply_time: 1672760
request: POST /joomla/administrator/index.php HTTP/1.1
request_ack_time: 51724
request_time: 0
```

Successful Login



# Unauthorized Access ☹️

What happened next



# Post Exploit

## Setting the time range

The screenshot shows the Splunk search results interface. At the top, there are controls for 'List', 'Format', and '20 Per Page'. Below this is a table with columns 'i', 'Time', and 'Event'. The first row shows a time range '10/08/2016 21:48:05.858' highlighted with a pink box. A pink arrow labeled '1' points to this box. A dialog box titled '\_time' is open in the foreground. It has three options: 'Before this time', 'After this time' (which is selected and highlighted with a pink box), and 'At this time'. A pink arrow labeled '2' points to the 'After this time' option. Below these options is a 'Nearby Events' section with a dropdown for '+/-', a value of '5', a unit of 'second(s)', and an 'Apply' button. The background shows a list of search results with various fields like 'client\_rtt\_sum', 'connection\_type', 'cookie', 'cs\_cache\_control', 'cs\_content\_length', 'cs\_content\_type', and 'cs\_version'.

# 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
```

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

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

Time	Event
10/08/2016 22:52:47.035	<pre>{   "endtime": "2016-08-10T21:52:47.035555Z",   "timestamp": "2016-08-10T21:52:45.437445Z",   "accept": "text/html, application/xhtml+xml, */*",   "accept_language": "en-US",   "content-length": 94,   "dest_ip": "192.168.250.70",   "dest_mac": "00:0C:29:C4:02:7E",   "dest_port": 80,   "duplicate_packets_in": 52,   "duplicate_packets_out": 52,   "http_method": "POST",   "http_status": 200,   "http_version": "1.1",   "url": "http://192.168.250.70:80/192.168.250.70.exe" }</pre>

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
2016-08-10 23:19:14	C:\Program Files (x86)\PHP\v5.5\php-cgi.exe	cmd.exe /c "dir 2&gt;&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;&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;&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;&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;&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 innotbatman.jpg 2&gt;&1"
2016-08-10 23:20:33	C:\Windows\SysWOW64\cmd.exe	\??\C:\Windows\system32\conhost.exe 0xffffffff

**Innotbatman.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 ▾

- a http\_content\_type 1
- a http\_method 1
- a index 1
- # linecount 1
- # missing\_packets\_in 1
- # missing\_packets\_out 1
- a network\_interface 1
- # packets\_in 2
- # packets\_out 2
- a punct 2
- # reply\_time 6
- a request 4
- # request\_ack\_time 7
- # request\_time 3
- # response\_ack\_time 5
- # response\_time 3
- # cache\_control 1
- # server\_rtt\_packets 2
- # server\_rtt\_sum 7
- a site 2
- a splunk\_server 1
- a src\_headers 4

request

4 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

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 HTTP/1.1	2	28.571%
GET /core/extensions/com_joomlaupdate.xml HTTP/1.1	1	14.286%

client\_rtt: 202  
client\_rtt\_packets: 1  
client\_rtt\_sum: 202  
cs\_version: 1.0  
data\_center: sfv1

More Badness!

1

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

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
```

Chpt6 - Search 1

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

100,500 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000) No Event Sampling

Events (100,500) Patterns Statistics (4) Visualization

20 Per Page Format Preview

host	IIS	IIS	NT	NT	NT	NT	WAYNECORPINC\Administrator	WAYNECORPINC\bc	Window Manager\DW-3	admin	NULL
splunk-02	0	0	0	0	0	0	0	0	0	344	0

Save As Dashboard Panel

Dashboard: New

Dashboard Title: Security Operations

Dashboard ID: security\_operations  
Can only contain letters, numbers and underscores.

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

# 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

splunk>enterprise App: Security4Rookies

Administrator Messages Settings Activity Help Find

Search Datasets Reports Alerts Dashboards Network Diagram Ready Made Searches

App Security4Rookies

### Chpt6 - Search 2

Save Save As View Close

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

✓ 41,949 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000) No Event Sampling

Events (41,949) Patterns Statistics (24) Visualization

Cluster Map Format Trellis

latitude	longitude	185.10.200.26	23.22.63	40.80.148.42
39.04730	-77.47449			1

Dashboard ☐ New ☒ Existing

Security Operations

Panel Title Unexpected Logon Sources

Panel Powered By ☒ Inline Search ☐ Report

Drilldown? No action

Panel Content ☒ Statistics ☐ Cluster Map

Cancel Save

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
```

splunk>enterprise App: Security4Rookies

Search Datasets Reports Alerts Dashboards Network Diagram Ready Made Searches

New Search

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

23,936 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000) No Event Sampling

Events (23,936) Patterns **Statistics (247)** Visualization

20 Per Page Format Preview

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

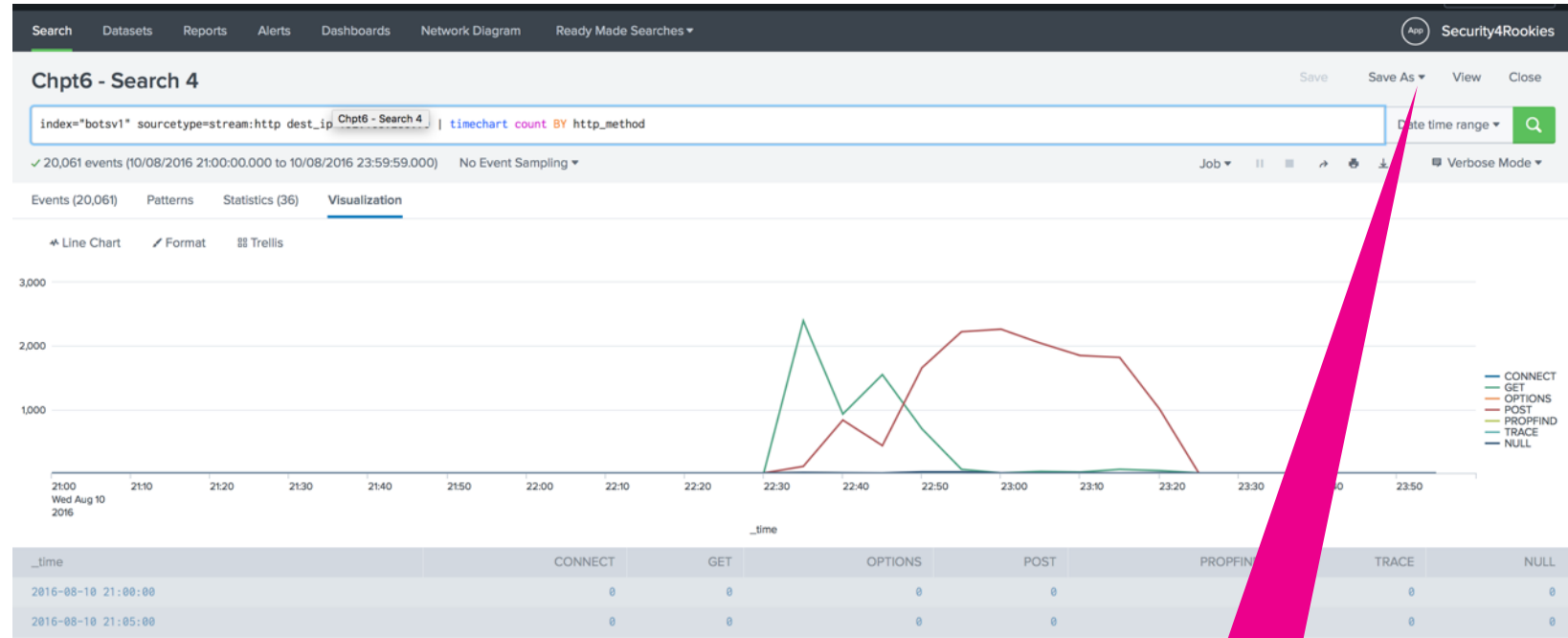
# Dashboards

## 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

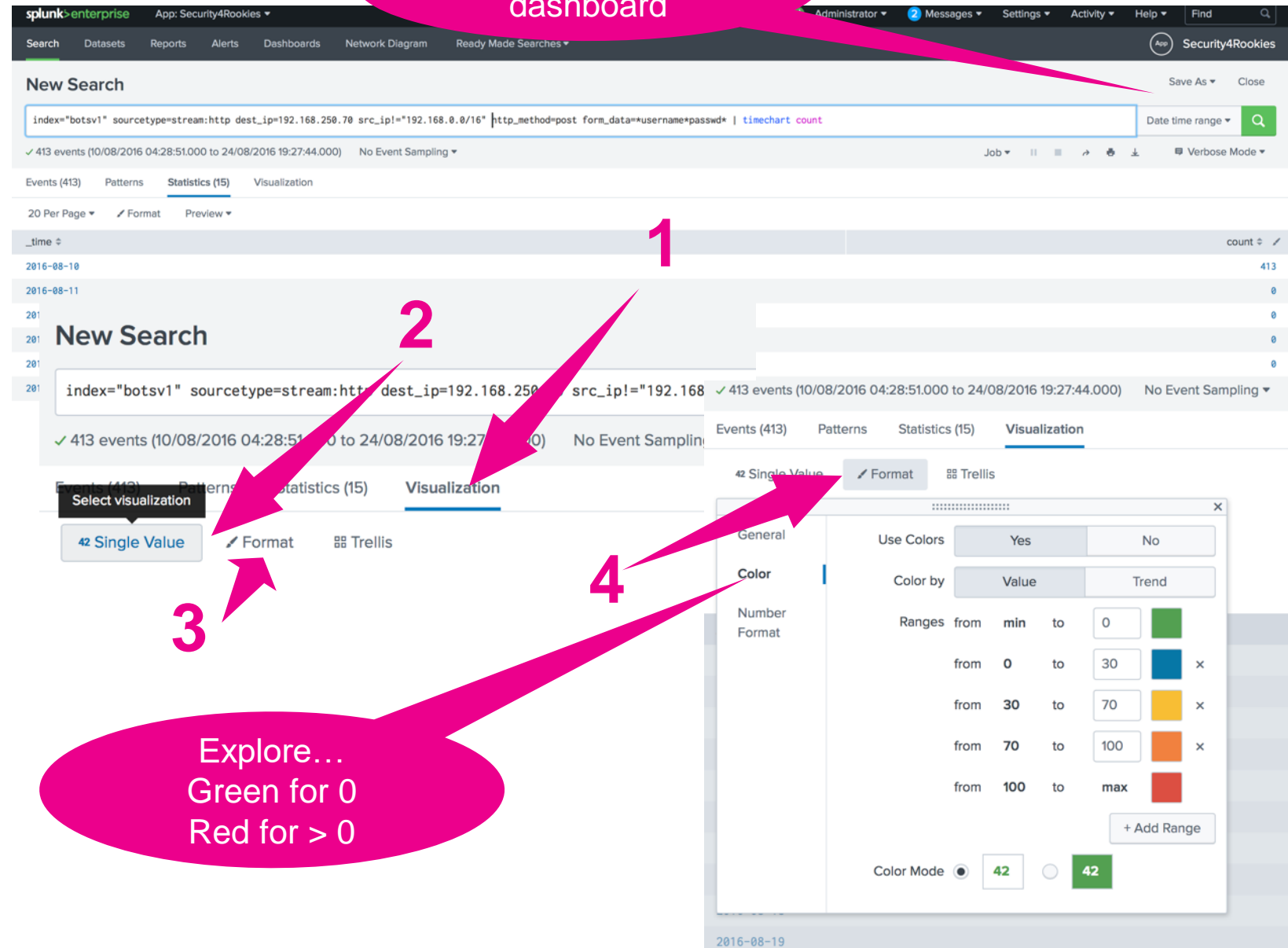
# Dashboards

## 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

Search | Datasets | Reports | Alerts | Dashboards | Network Diagram | Ready Made Searches

### 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

### 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

Select Visualization

42 Single Value | Format | Trellis

Explore...  
Green for 0  
Red for > 0

General

Use Colors ☒ Yes ☐ No

Color by ☒ Value ☐ Trend

Number Format

Ranges from min to 0

from 0 to max

+ Add Range

Color Mode ☐ 42 ☒ 42



# Dashboards

Visualizations

Interactive

splunk>enterprise App: Security4Rookies ▾

Search Datasets Reports Alerts Dashboards Network Diagram Ready M

## Search

ent **Dashboards**  
Dashboards include searches, visualizations, and inp

No E 2 Dashboards

i	Title ^
>	Network Diagram
>	Security Operations

Search Datasets Reports Alerts Dashboards Network Diagram Ready Made Searches ▾

**Security Operations** Edit Export ▾ ...

Password attempts per user

host ⇅	user ⇅	numPasswords ⇅
sp1unk-02	admin	344

# Dashboards

## Visualizations

Add time selector

The image shows a Splunk dashboard titled "Security4Rookies" with an "App" button. Below the title bar are "Edit", "Export", and a menu icon. A navigation bar at the top contains "Search", "Datasets", "Reports", "Alerts", "Dashboards", "Network Diagram", and "Ready Ma". The main content area is titled "Edit Dashboard" with tabs for "UI" and "Source". A "+ Add Panel" button and a "+ Add Input" dropdown are visible. The dropdown menu is open, showing options: "T Text", "Radio", "Dropdown", "Checkbox", "Multiselect", "Link List", "Time", and "Submit". A pink arrow labeled "2" points to the "Time" option. Another pink arrow labeled "3" points to the "Submit" option. Below the dropdown, a panel titled "Security Operations" is shown. A pink arrow labeled "4" points to the panel's configuration icon. The configuration window is open, showing the "General" tab. The "Label" field is set to "Time Period" (indicated by pink arrow "5"). The "Search on Change" checkbox is unchecked. Under "Token Options", the "Token" field is set to "tok\_time" (indicated by pink arrow "6") and the "Default" is set to "All time". The window has "Cancel" and "Apply" buttons at the bottom.

# Dashboards

## Visualizations

Make panels react

Time Period

All time

Website logons from external IPs

No title

Edit search

42

Edit Search

Title

Search String

```
index="botstv1" 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
```

Run Search

Time Range

Use time picker

Shared Time Picker (tok\_time)

Auto Refresh Delay ?

Use time picker

Tokens

Refresh Indicator

Global

Cancel

Convert to Report

Apply

Repeat for all panels

# Dashboards

## Visualizations

### Changing Visualization Type

Diagram illustrating the steps to change the visualization type of a dashboard panel:

- Step 1:** Click the visualization icon (grid) in the top right corner of the panel header.
- Step 2:** Select the desired visualization type from the "Splunk Visualizations" menu. In the example, the "Column Chart" is selected.
- Step 3:** Configure the visualization settings in the configuration panel. In the example, the "Stack Mode" is set to "stacked 100%".

The diagram shows a dashboard titled "Password attempts per user" with a table of data. The table has columns for host, user, and password attempts. The data is as follows:

host	user	password attempts
we11-	APPPOOL\DefaultAppPool	1
we811	APPPOOL\joomla	1
we90-	NT\AUTHORITY\USER	1
	NT\AUTHORITY\LOCAL SERVICE	1
	NT\AUTHORITY\NETWORK SERVICE	1
	NT\AUTHORITY\SYSTEM	1
	WAYNECORPINC\Administrator	0
	WAYNECORPINC\joomla	1
	Window Manager\DWM-3	0

# Dashboards

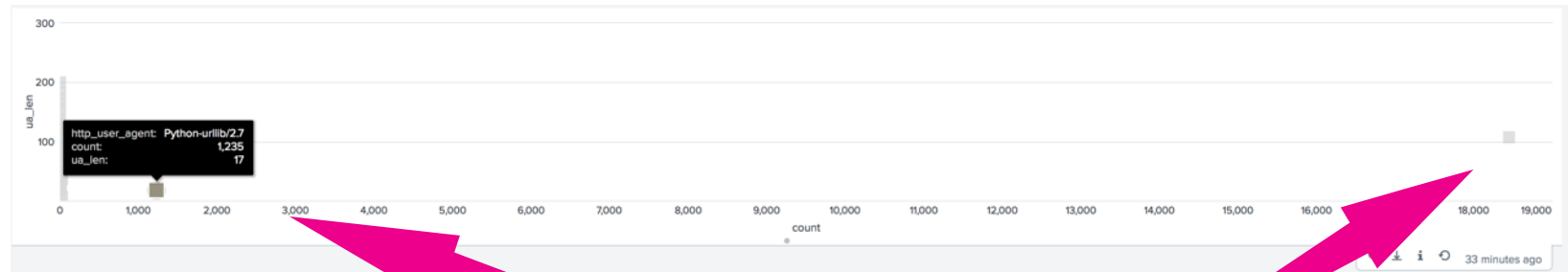
## Visualizations

## Bonus Challenge

Change http\_user\_agent panel to a scatter chart

YUK! – Wrong type of vis for the data!

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



Rare features stand out with good visualizations

# Dashboards

## Visualizations

## Interactive Filtering

The screenshot shows the Splunk dashboard editor interface. At the top, there is a navigation bar with links: Search, Datasets, Reports, Alerts, Dashboards, Network Diagram, and Ready. Below this, the 'Edit Dashboard' tab is active, with sub-tabs for 'UI' and 'Source'. The main area displays a dashboard titled 'Security Operations' with a description 'No description'. A 'Time Period' filter is set to 'All time'. A visualization titled 'Website logons from external IPs' is shown. A dropdown menu is open, listing various input types: T Text, Radio, Dropdown, Checkbox, Multiselect, Link List, Time, and Submit. A pink arrow labeled '1' points to the '+ Add Input' button. A pink arrow labeled '2' points to the 'Dropdown' option in the menu. A pink arrow labeled '3' points to the 'Label' field, which contains the text 'User'. A pink arrow labeled '4' points to the 'Token ?' field, which contains the text 'tok\_user'. A tooltip below the token field reads 'The default value of the input.' Other fields include 'Search on Change' (unchecked), 'Default ?' (Set to 'Select...'), 'Initial Value ?' (Set to 'Select...'), and 'Clear Selection' buttons. At the bottom, there are 'Cancel' and 'Apply' buttons.

1

2

3

4

Scroll Down





# Dashboards

## Visualizations



## Continued

Static Options


Name	Value
 ALL	* 


[+ Add New](#)

Dynamic Options

Content Type  

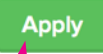
Search String `| inputlookup user_list |  
sort user`

[Run Search](#) 

Last 24 hours 

Field For Label?

Field For Value



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

General

Token Options

Static Options

+ Add New

Dynamic Options

Content Type

Search String

Run Search

Last 24 hours

Field For Label ? user

Field For Value ? user

Cancel

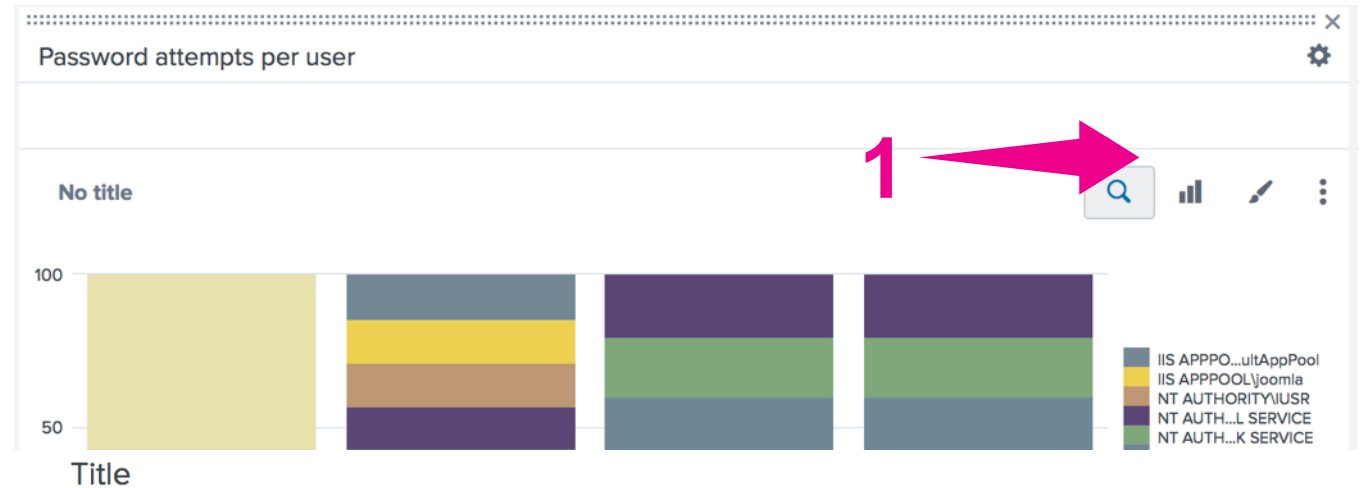
Apply

11

# Dashboards

## Visualizations

Substitute tokens into a dashboard search



ADD

"search user=\$tok\_user\$ |"

# And..... Breathe!



# Splunk Resources

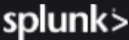
# Resources

## 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-CAAH9U>
- 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




Register

## 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!



App: L. ▾ Splunk ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Overview ▾ Web-Shells ▾ Supplemental Material ▾ Search

Investigating MACCDC

### Introduction

Export ▾ ...

#### 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: \*

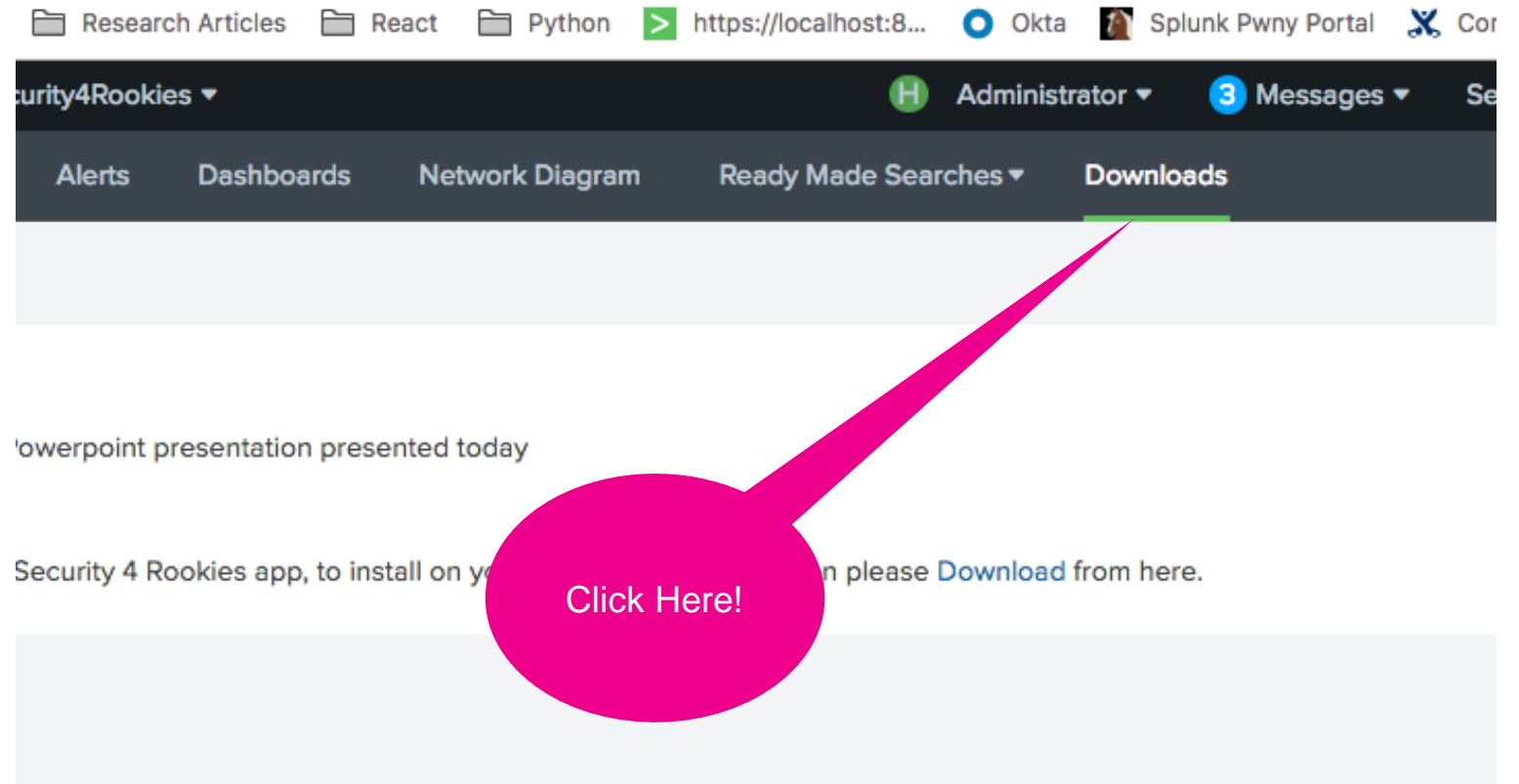
First Name: \*

Last Name: \*

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

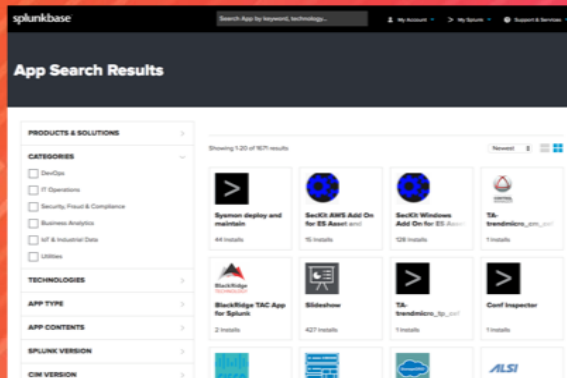
# Today's Content

## Download and play

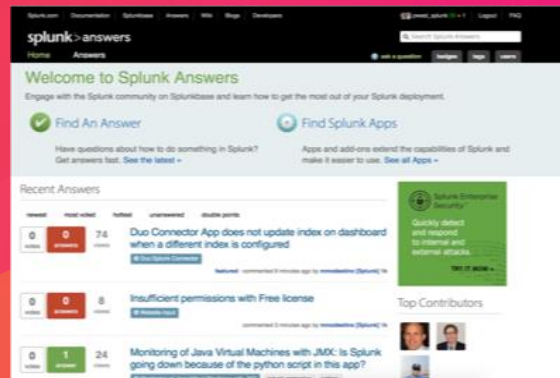


# Thriving Community

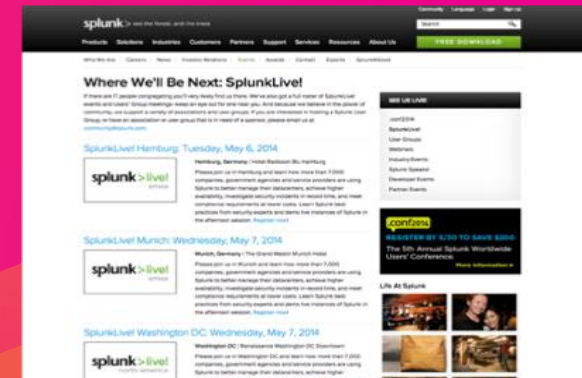
## Splunkbase



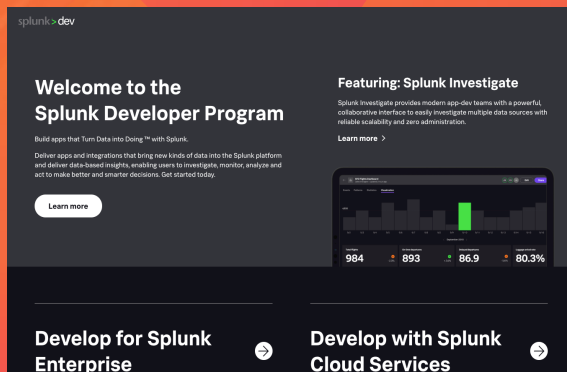
## Splunk Answers



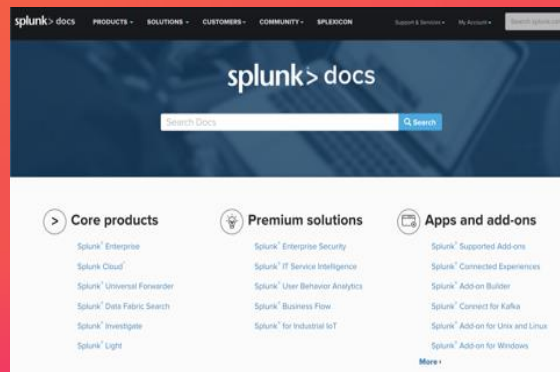
## Splunk Events



## Developer Resources



## Documentation



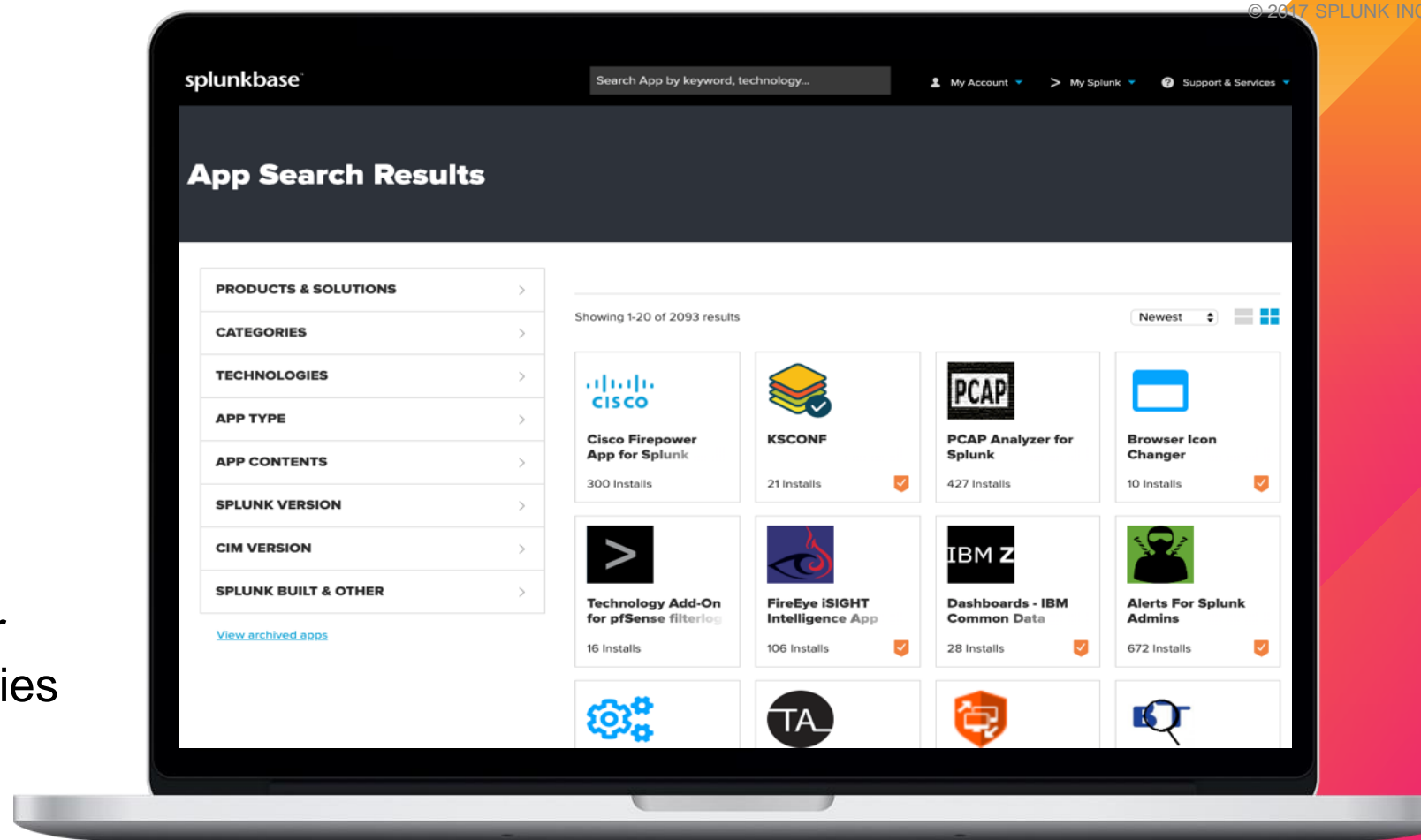
## Education



# 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!

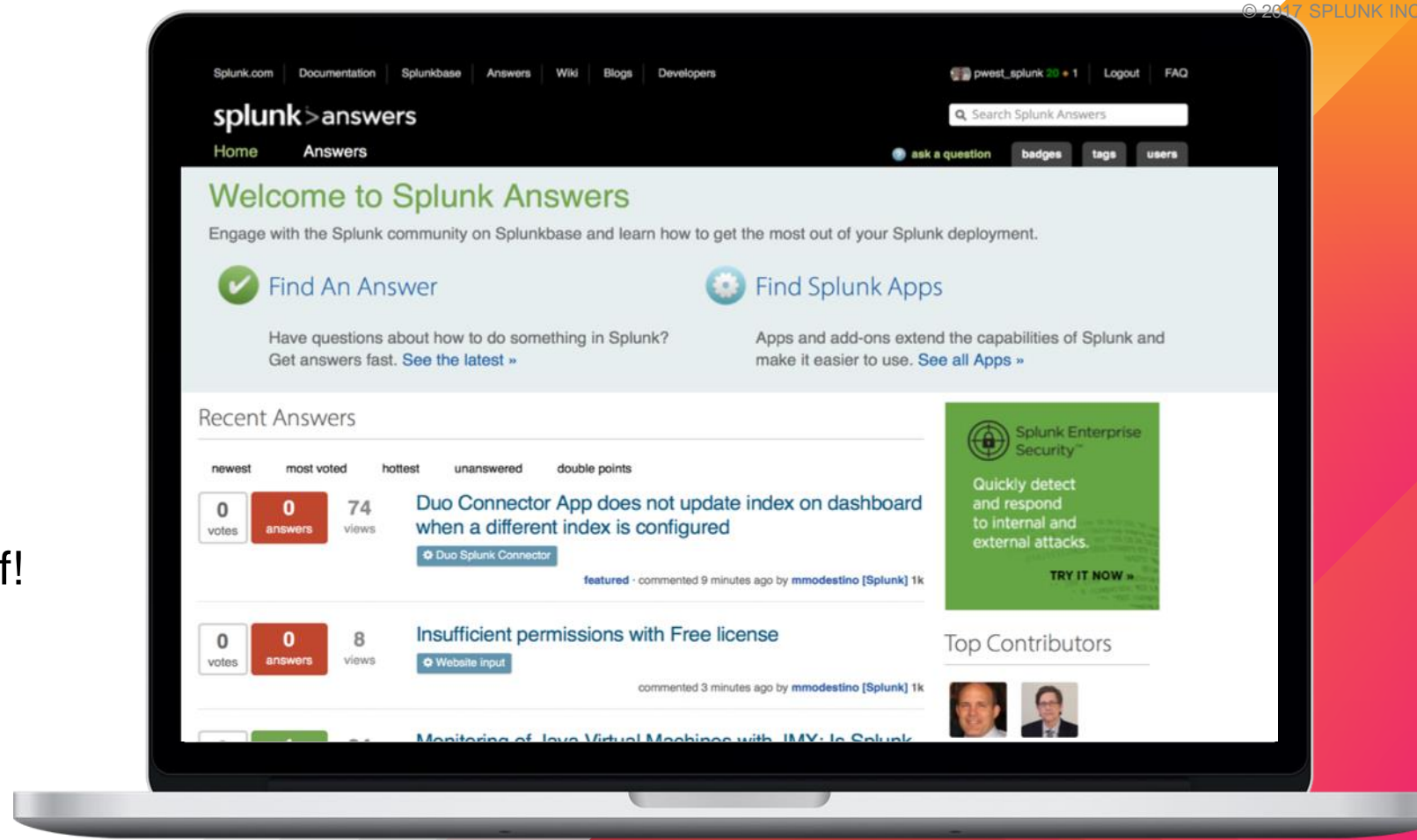




# Splunk Answers

<https://answers.splunk.com>

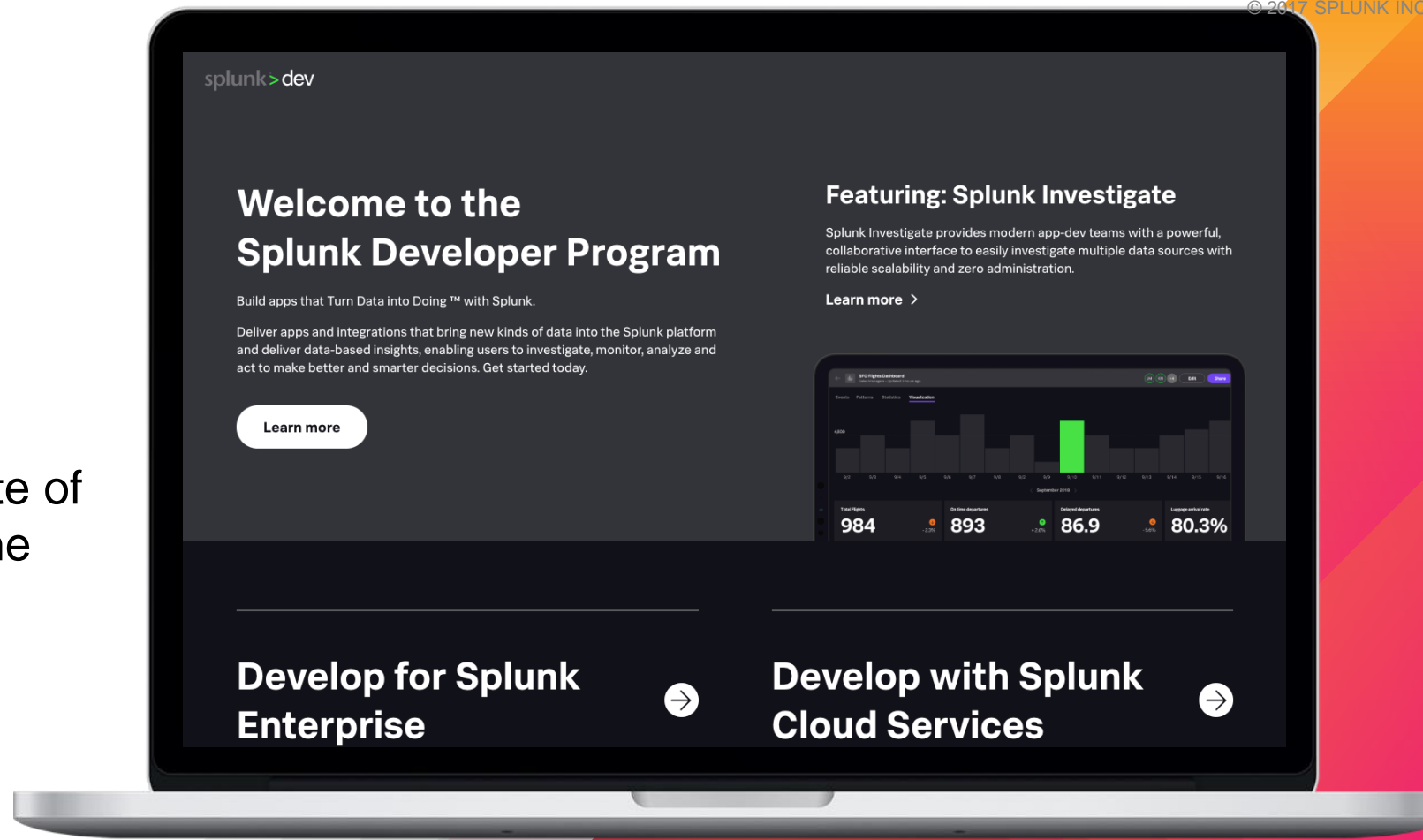
- > Get answers to your questions from Splunk 'know-it-all's, or share what you've learned to achieve know-it-all status yourself!
- > Engage with the Splunk community and learn how to get the most out of your Splunk deployment.



# 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

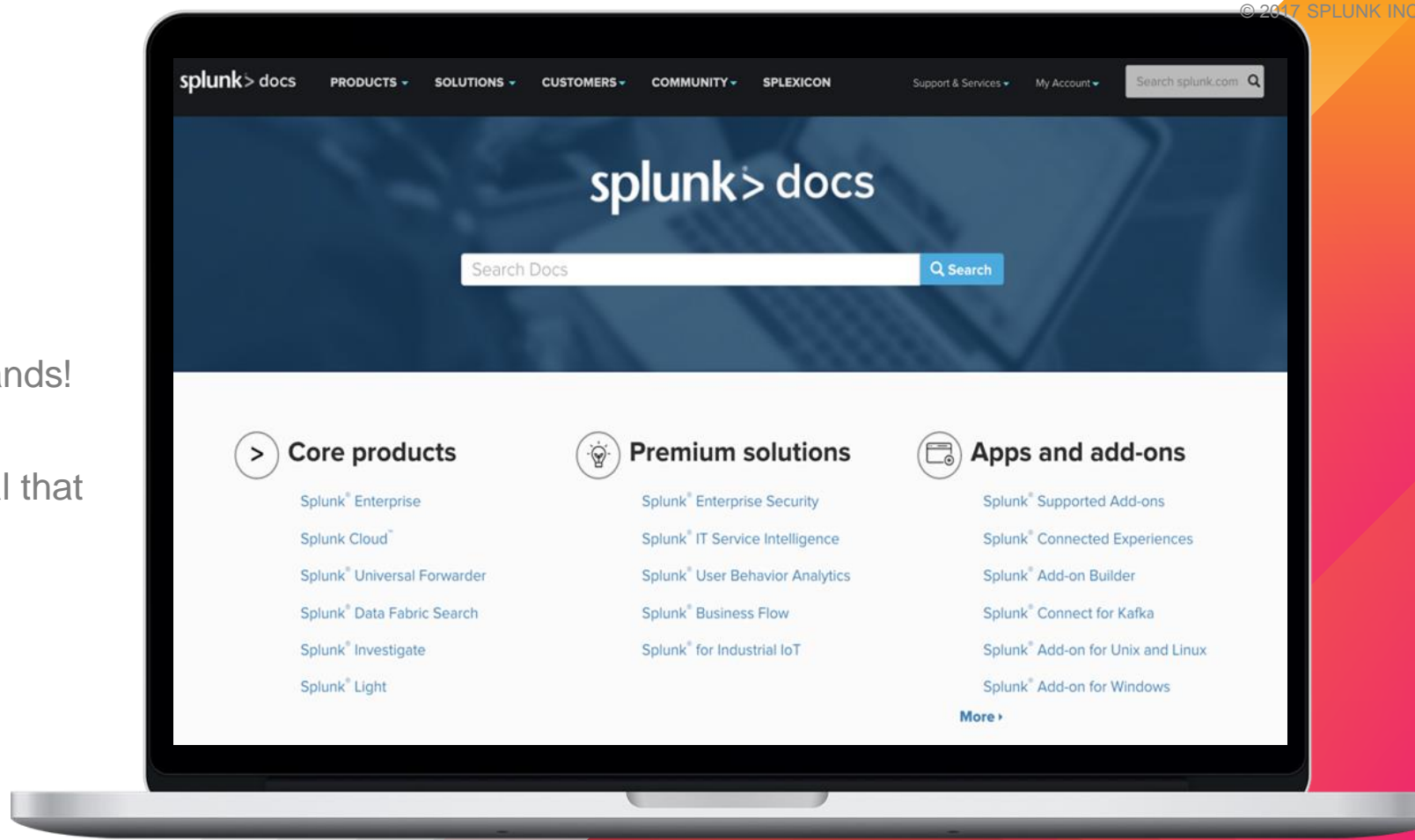




# Documentation

<https://docs.splunk.com>

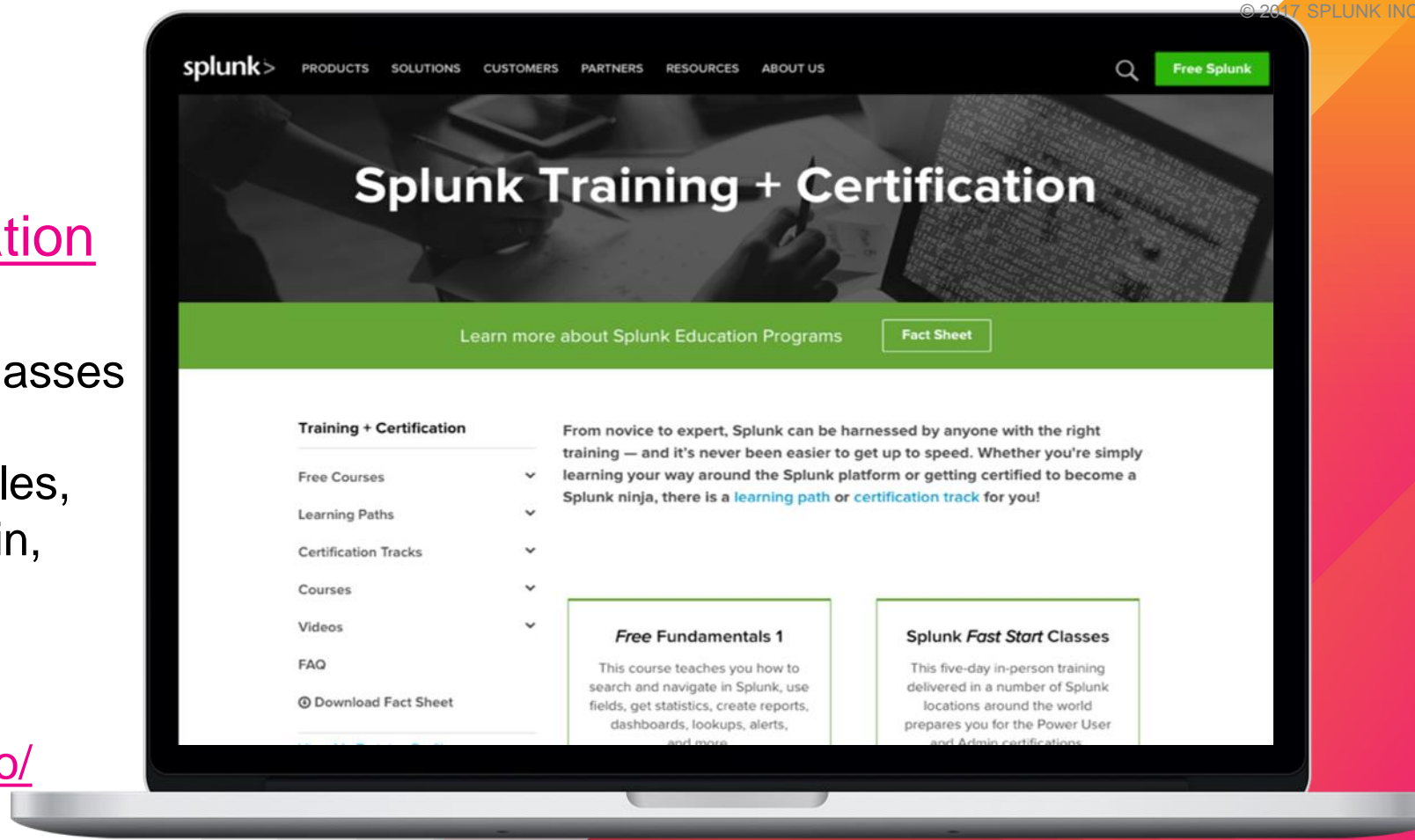
- > Splunk reference – Learn the commands!
- > Tutorials – Check out the search tutorial that even includes sample data to play with!
- > Use cases
- > References
- > Procedures/guides – installing, upgrading
- > And more!



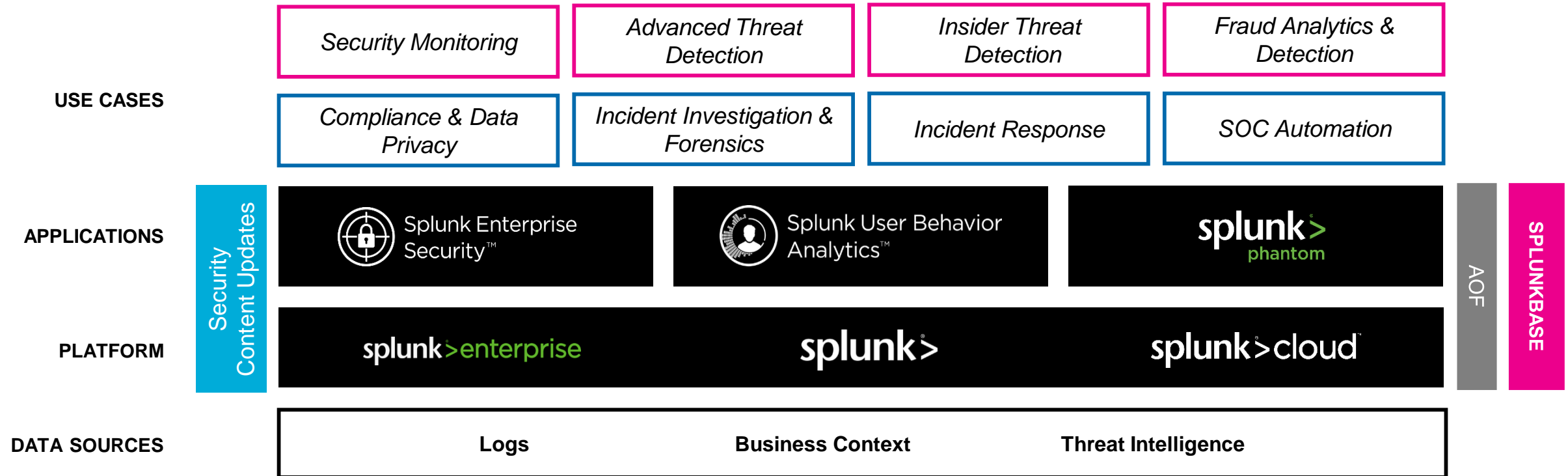
# Education

<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/demo/>
- > Free education!  
**FREE: Online Splunk Fundamentals 1 course**



# Security Operations Suite

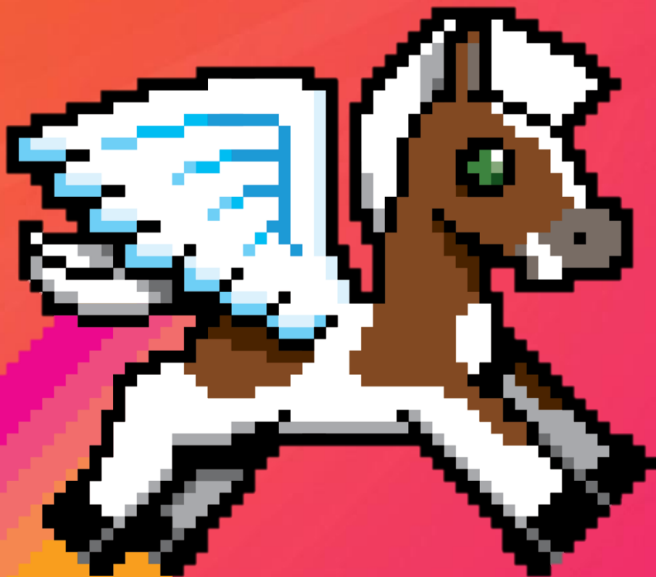


# Feedback

Just One More Thing



# Thank You



splunk® > turn data into doing™