

# Splunk4Rookies - Security



splunk>



# Forward-Looking Statements



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

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

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

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. Splunk, Splunk> and Turn Data Into Doing 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. © 2023 Splunk Inc. All rights reserved.

# Please introduce yourself!

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





# Workshop Agenda

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

# There's a Lot More to Splunk

- Clustering
- Data Models
- Alerting
- Pivot
- SDKs
- APIs
- DB Connect

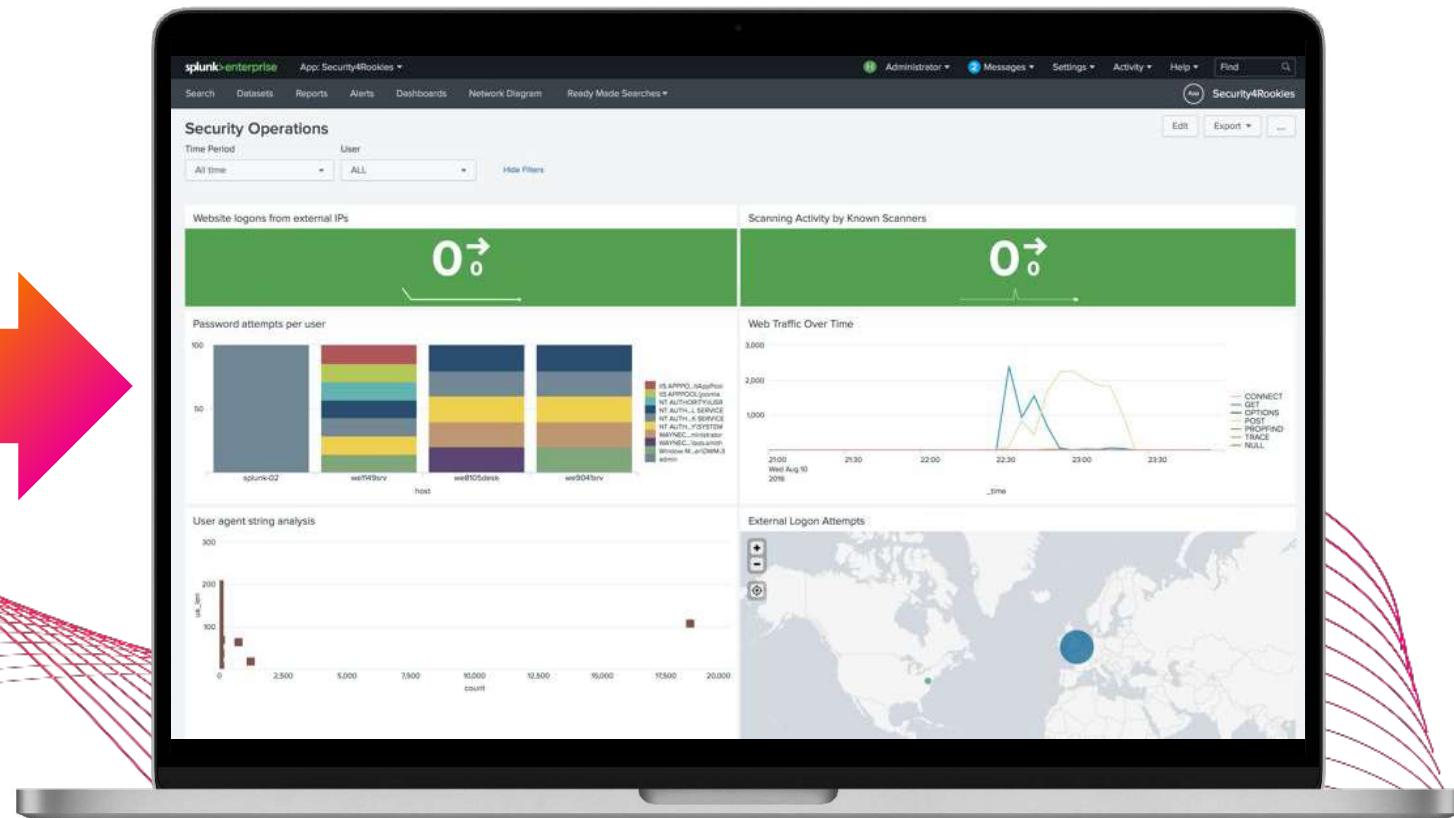
- Advanced Searches
- SOAR
- Machine Learning (ML)

- Splunk Stream
- Deployment Server
- Federated Search
- Metrics

- Custom Visualisations
- HTTP Event Collector (HEC)
- Data Filtering
- Transformations
- Architecture

- Report Acceleration
- Common Information Model (CIM)
- Containers
- Best Practices
- And much more...

# Objective for Today



splunk>



REGISTRATION

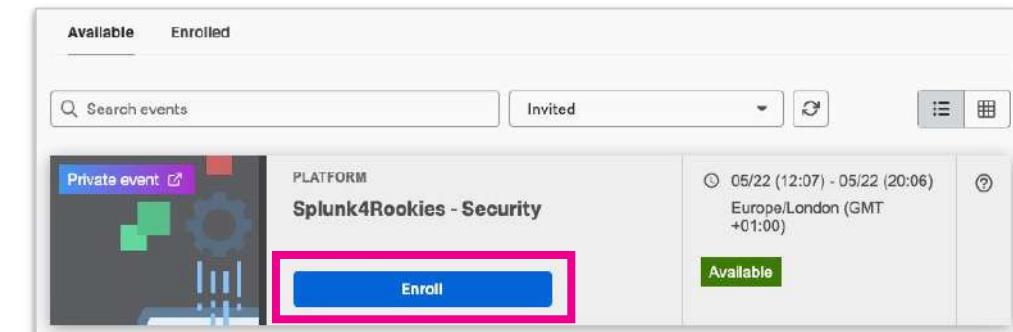
5 MINS

# Enroll in Today's Workshop

## Tasks

1. Get a splunk.com account if you don't have one yet:  
<https://splk.it/SignUp>
2. Enroll in the Splunk Show workshop event:  
<https://show.splunk.com/event/<eventID>>
3. Download a copy of today's slide deck:  
<https://splk.it/S4RS-Attendee>

## Goal

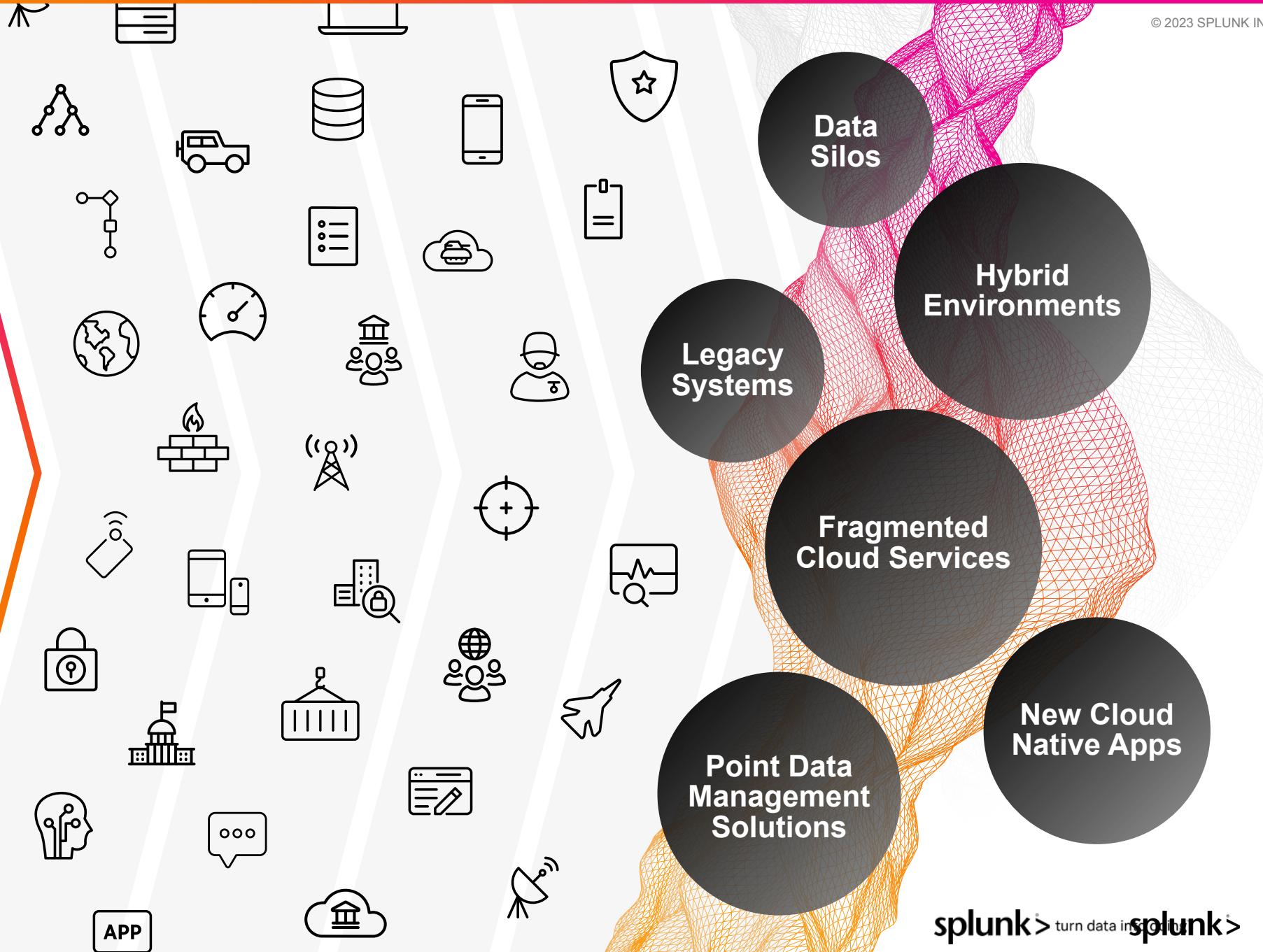


Enroll in today's event

# Data is your Competitive Advantage

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

# Turning Real-time Data Into Action is Hard



# The Power of Splunk

Delivering Unified Security and Observability

## See

**End-to-end visibility**

No sampling or blind spots

## Act

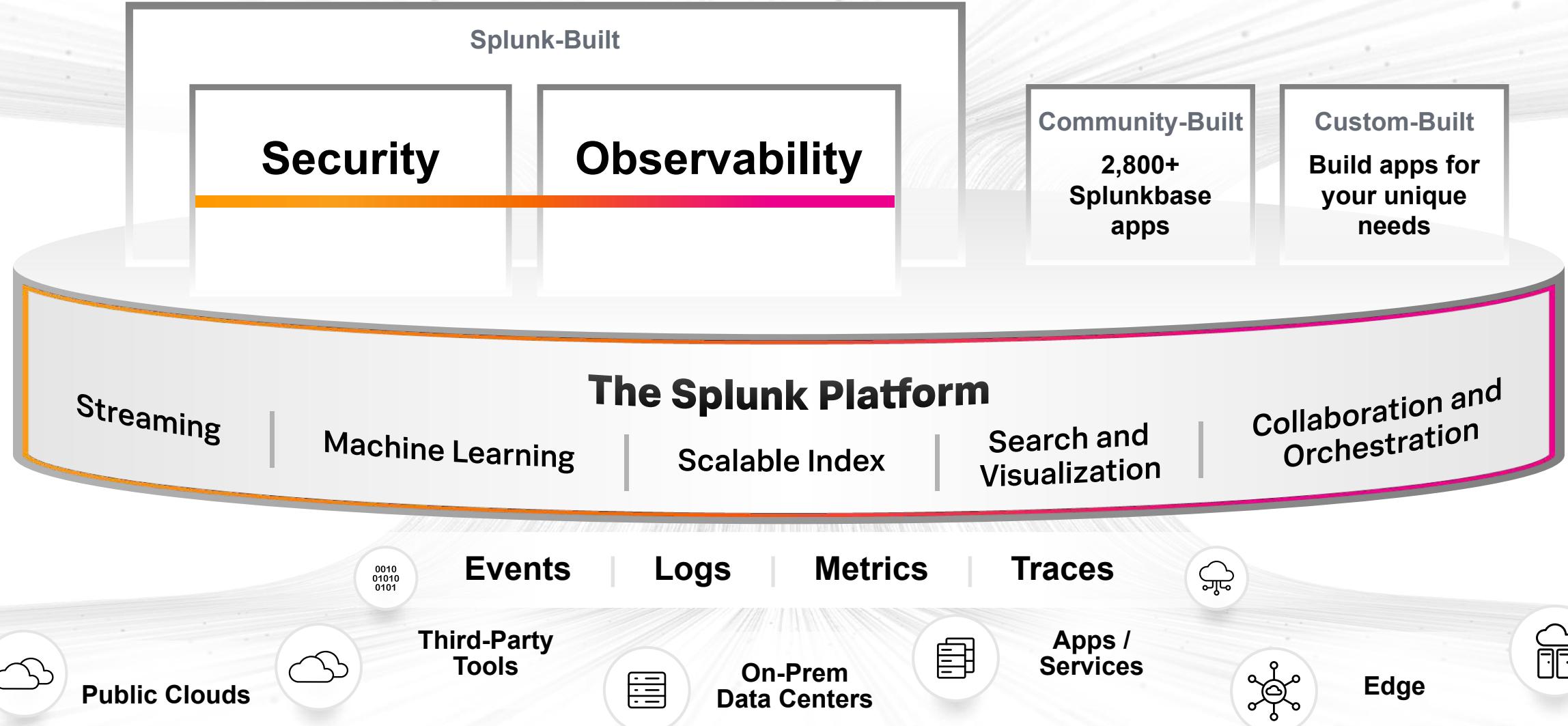
**Investigate** across massive data sets and take **action** fast

## Extend

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



# The Unified Security and Observability Platform

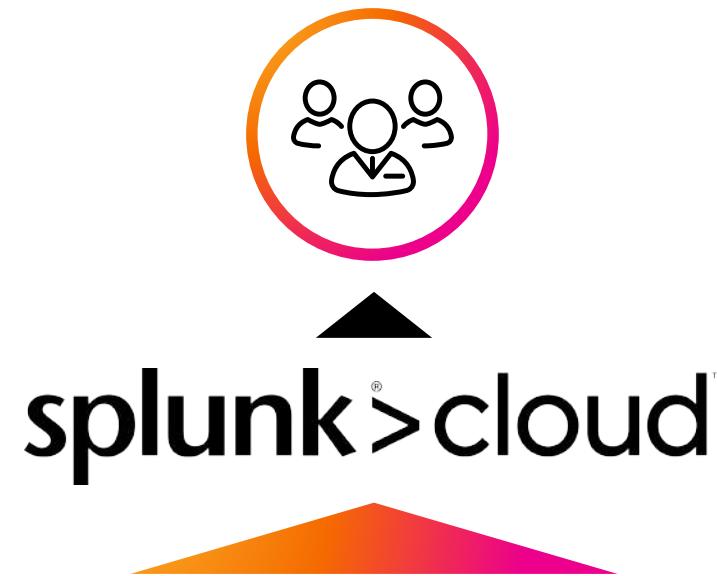


# Splunk as a Service

Fastest time to value | Minimum Infrastructure | Maximum Value

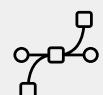
## 3 Simple Steps

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



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

## Flexible options for data collection and forwarding



Wire Data



API



SDKs



HEC



HTTP



TCP/UDP



RDBMS



Containers



Apps



Cloud Services



OpenTelemetry

Splunk  
Forwarders

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

splunk>

# Splunk for Security

Unifying data, analytics, and operations

## SPLUNK MISSION CONTROL

Splunk  
SIEM  
(ES & UBA)

Splunk  
SOAR  
(Phantom)

Splunk  
Security Apps  
(SSE & InfoSec)

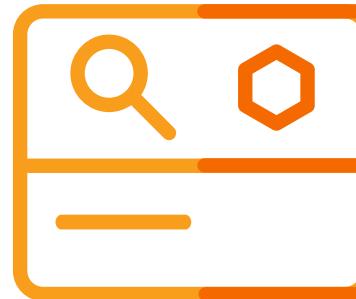
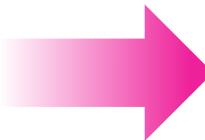
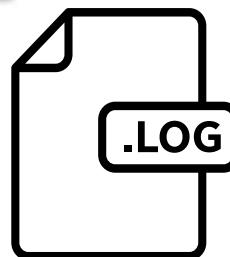
Future Splunk  
Solutions &  
3<sup>rd</sup>-Party  
Tools

splunk®

Data Sources  
Logs, Business Context,  
Threat Intelligence

# Today's Environment

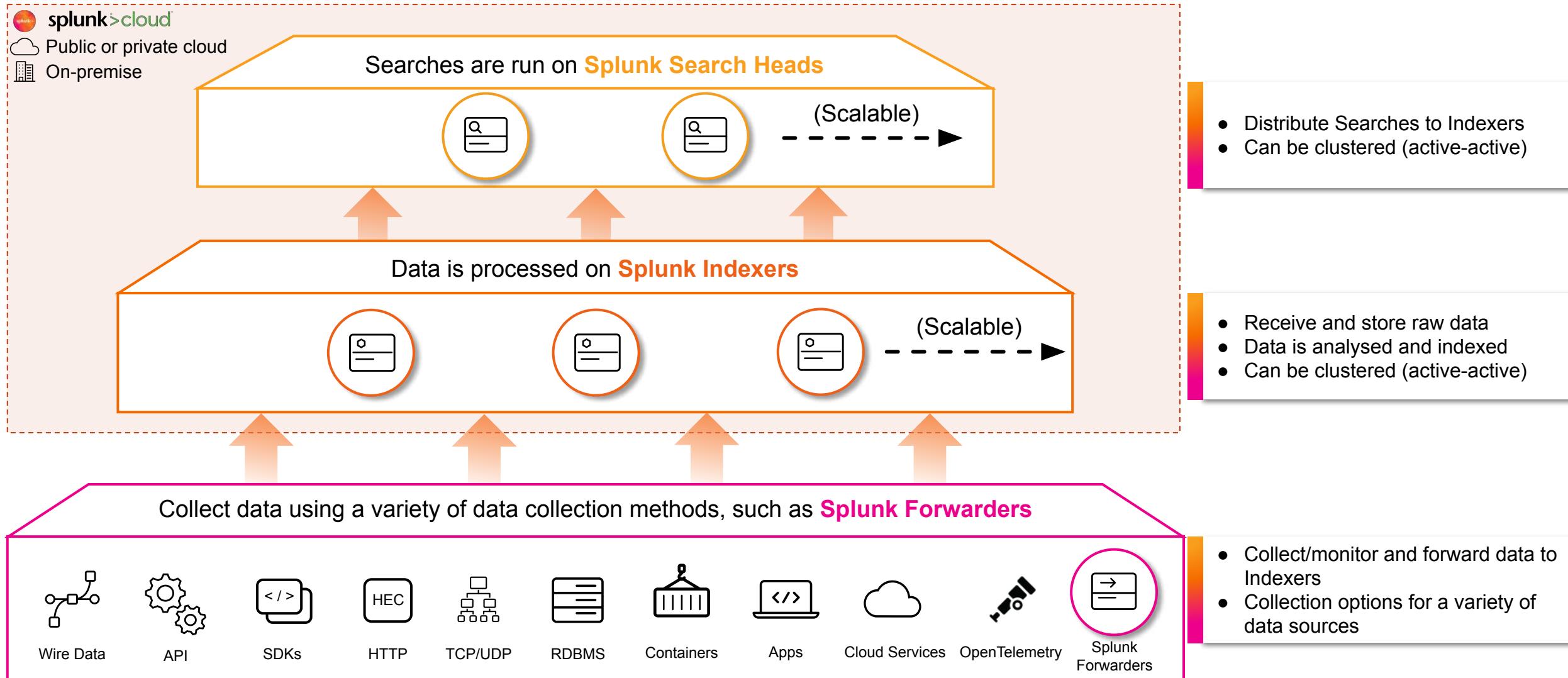
Sample data to play with



Indexer & Search Head  
combined in a single instance

# Scales to Petabytes Per Day

Enterprise-Class Scale, Resilience and Interoperability



# What is a Splunk Universal Forwarder?

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



imreallynotbatman.com

# Security Data and Searches

For Security People



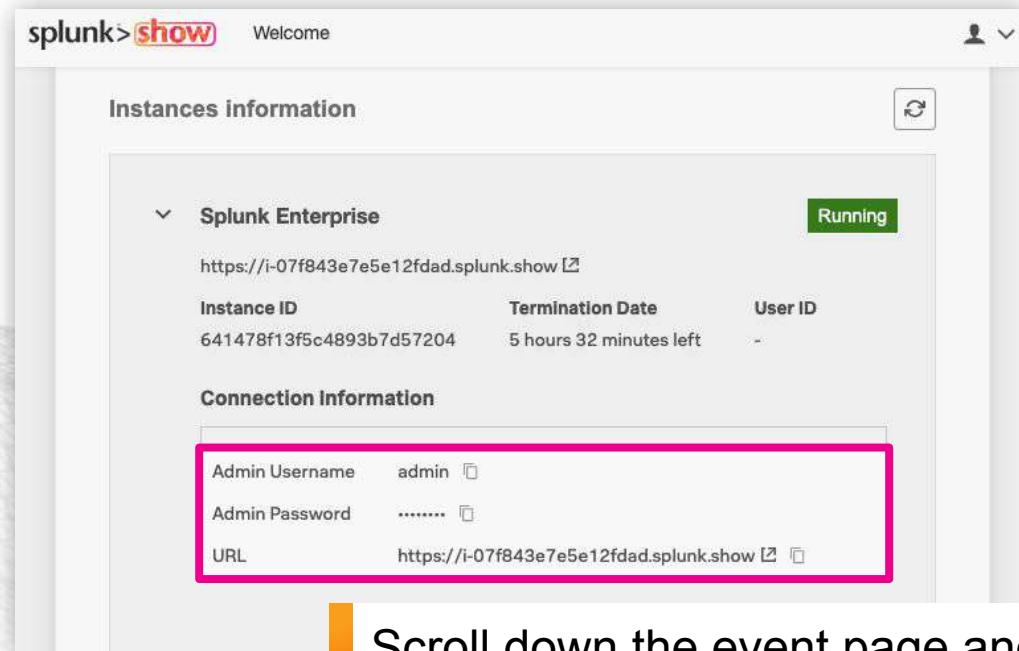


# Let's Go!

splunk>

# Login to Splunk

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



The screenshot shows the Splunk Show event page with the following details:

- Instances information:** Splunk Enterprise (Running)
- Instance ID:** https://i-07f843e7e5e12fdad.splunk.show
- Termination Date:** 5 hours 32 minutes left
- User ID:** -
- Connection Information:**
  - Admin Username: admin
  - Admin Password: ..... (redacted)
  - URL: https://i-07f843e7e5e12fdad.splunk.show

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

Log in to your Splunk instance



**Username: admin**  
**Password: changeme**



# Search Basics

Using SPL &  
Navigating the Splunk  
Search Bar

splunk>

# Search Basics

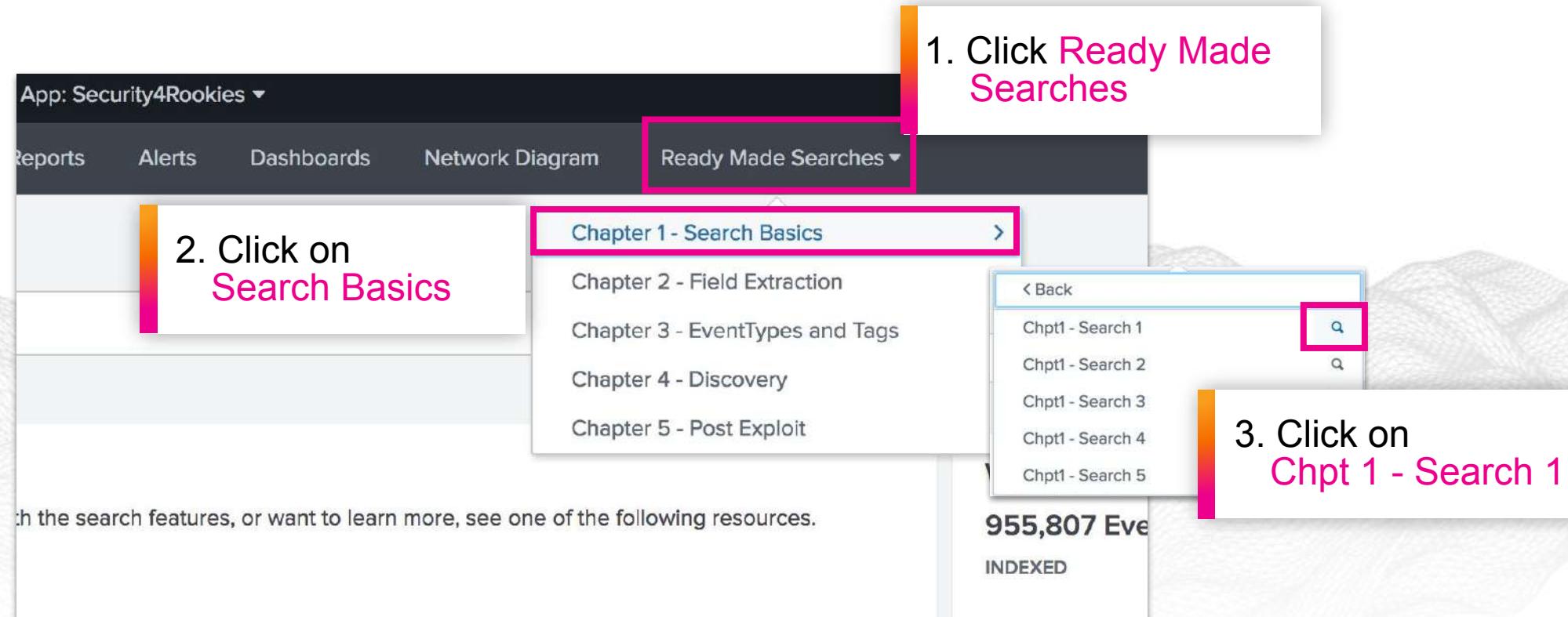
## Rules for the Workshop

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



# The Easy Button

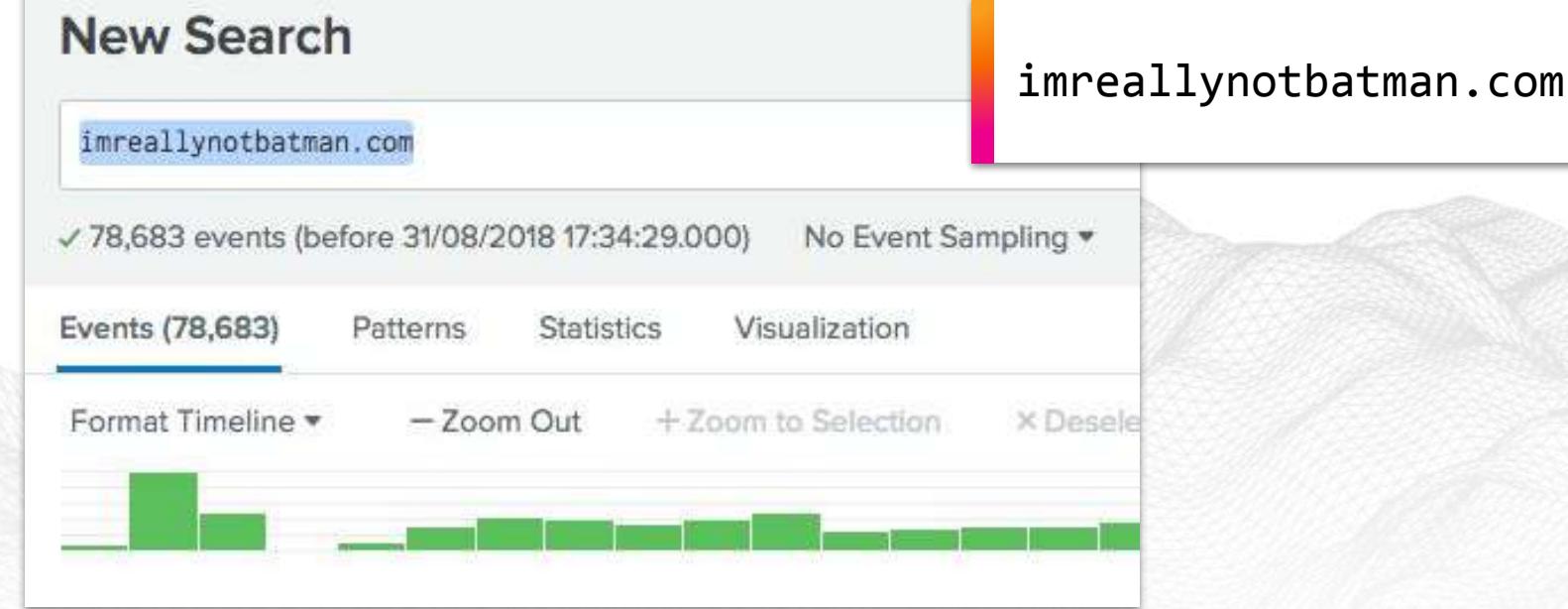
All lab searches have been pre-written for you



# Search Basics

## Chpt 1 - Search 1

### Literal Strings

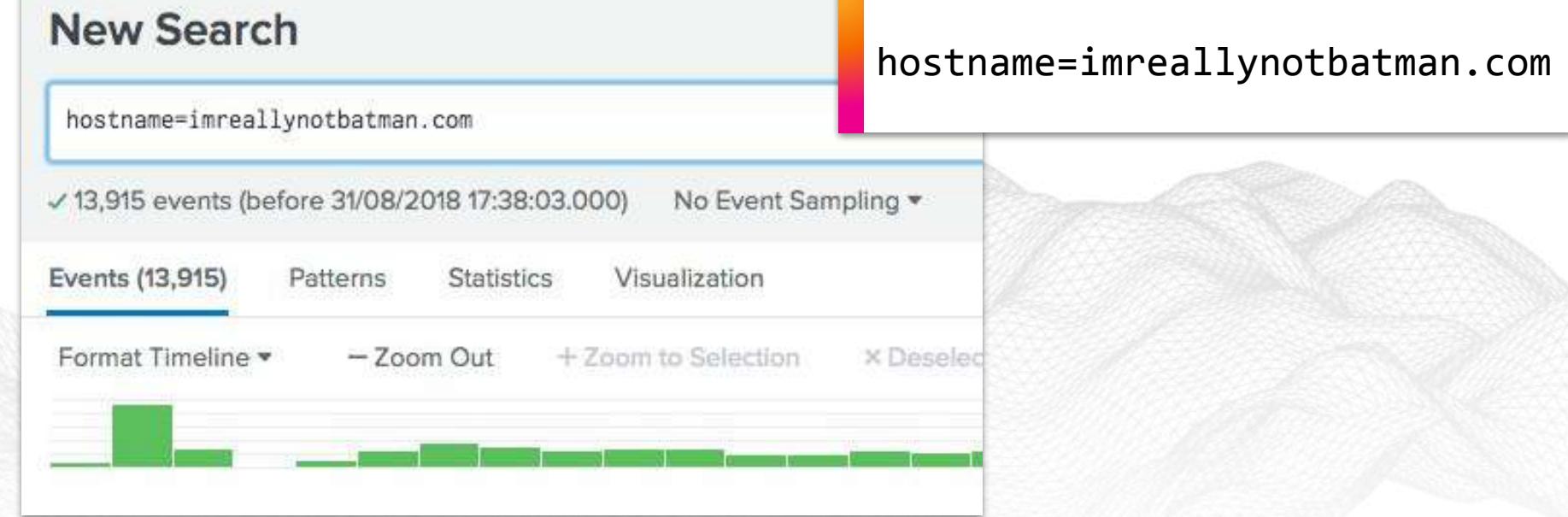


# Search Basics

## Chpt 1 - Search 2

### key=value pair matching

<u>Other Options</u>	
=	equals
!=	not equal to
>	greater than
<	less than
>=	greater or equal
<=	less than or equal to

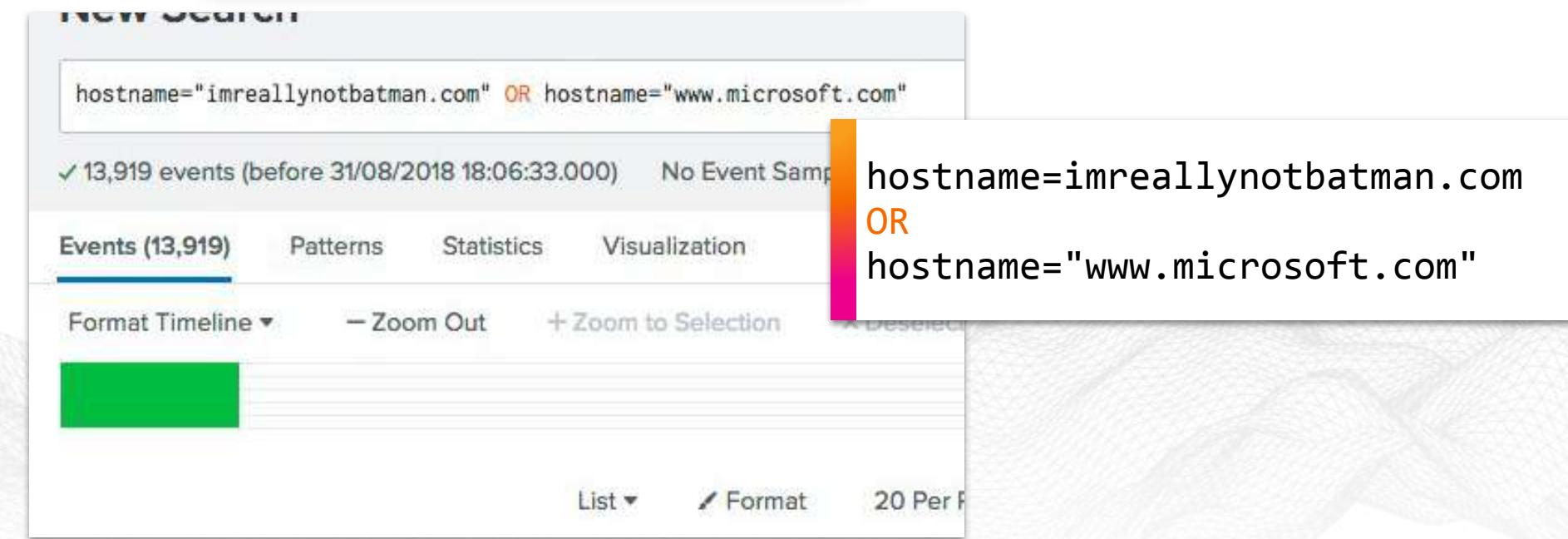


# Search Basics

## Chpt 1 - Search 3

### Using OR

**Remember Case**  
hostname="microsoft.com"  
**NOT** the same as  
HOSTNAME="microsoft.com"



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

- Search Bar:** hostname="imreallynotbatman.com" **OR** hostname="www.microsoft.com"
- Results Summary:** ✓ 13,919 events (before 31/08/2018 18:06:33.000) No Event Sample
- Event View:** Events (13,919) | Patterns | Statistics | Visualization
- Timeline Controls:** Format Timeline ▾ | – Zoom Out | + Zoom to Selection
- Bottom Navigation:** List ▾ | Format | 20 Per Page

A vertical color bar on the left and right sides of the interface has a gradient from orange at the top to red at the bottom, with a white center section containing the search terms and the OR operator.

# Search Basics

## Chpt 1 - Search 4

### Use Wildcards

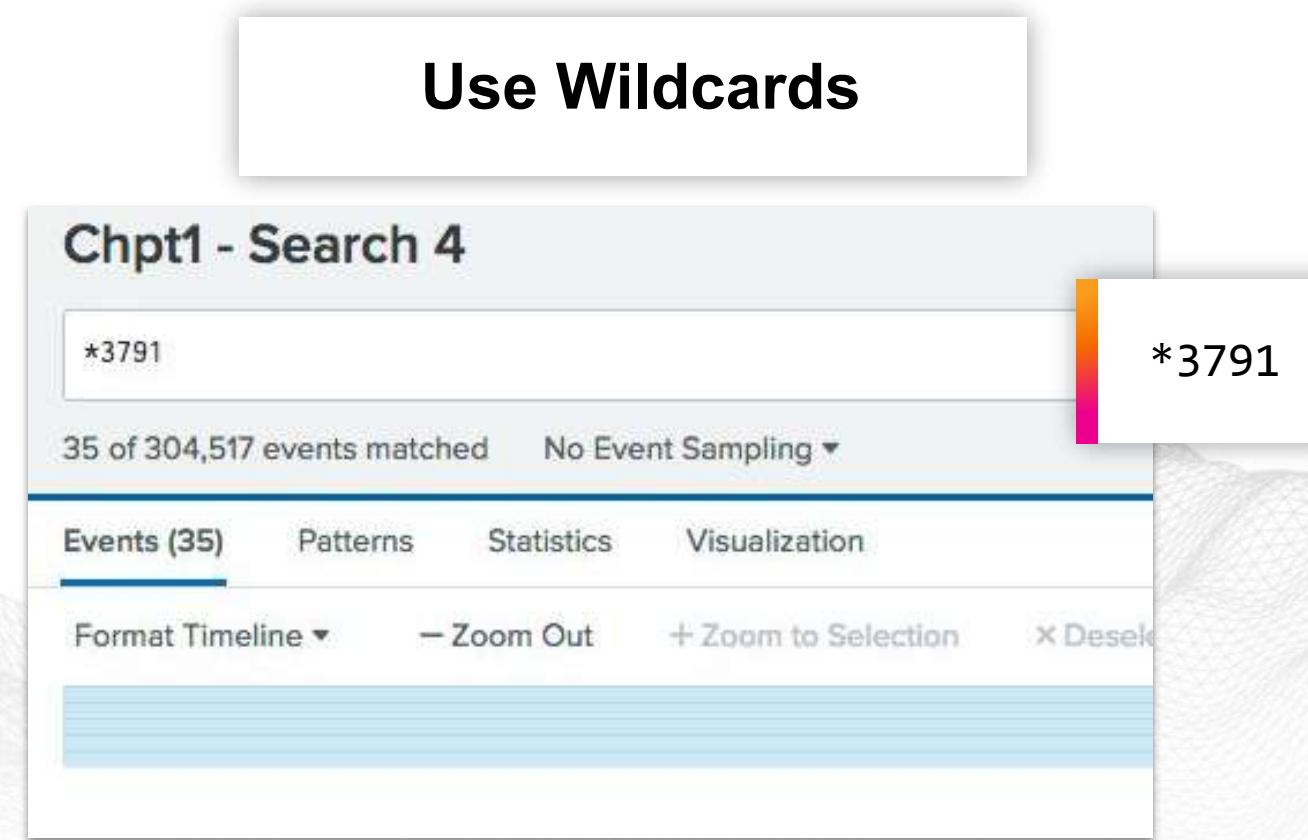
**Chpt1 - Search 4**

\*3791

35 of 304,517 events matched    No Event Sampling ▾

Events (35)    Patterns    Statistics    Visualization

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



# Search Basics

## Chpt 1 - Search 5

### Use Wildcards

The screenshot shows the Splunk search interface with the search term `3791*exe` entered in the search bar. The results panel indicates `11 events (before 31/08/2018 18:44:01.000)` and `No Event Sampling`. The `Events (11)` tab is selected. Below the search bar, there are controls for `Format Timeline`, `Zoom Out`, `Zoom to Selection`, and `Deselect`. At the bottom, there are buttons for `List`, `Format`, and `20 Per P`. A color scale bar on the right side of the results panel shows a gradient from yellow to red, with the text `3791*exe` next to it.

# Search Basics

## Chpt 1 - Search 6

### CIDR Matching

#### New Search

192.168.250.0/24

✓ 65 events (before 15/10/2018 15:18:29.000)

No Event Sampling

192.168.250.0/24

Events (65)

Patterns

Statistics

Visualization

Format Timeline ▾

– Zoom Out

+ Zoom to Selection

✖ Deselect

#### Also an Option

Could also key=value  
search

dest\_ip=192.168.250.0/24

# Search Basics

## Chpt 1 - Search 6

### CIDR Matching



# Splunk's Search Processing Language (SPL)

Search Terms

Commands

action=purchase | stats count by src\_ip | rename count as requests

Pipe character: Output  
of left is input to right

Functions

e.g. dest\_ip=192.168.250.70

i	Time	Event
>	24/08/2016 18:19:15.000	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><EventID>3</EventID><Version>5</Version><Level>4</Level><Task>SystemTime='2016-08-24T18:19:15.575273700Z' /><EventRecordID>3705233</Event><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we9041srv.wayne.corp<!--Uptime-->2016-08-24 18:20:05.127</Data><Data Name='ProcessGuid'>{46C7284<!--Image--><System><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='Ipv6'>false</Data><Data Name='SourceIp'>192.168.250.20</Data><Data Name='SourcePortName'>microsoft-ds</Data><Data Name='DestinationHostname'></Data><Data Name='DestinationPort'>64108</Data><Data Name='Host'>we9041srv</Data><!--source-->source = WinEventLog:Microsoft-Windows-Sysmon/Operational
>	24/08/2016 18:04:15.000	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><EventID>3</EventID><Version>5</Version><Level>4</Level><Task>SystemTime='2016-08-24T18:04:15.604356700Z' /><EventRecordID>3701741</Event><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we9041srv.wayne.corp<!--Uptime-->2016-08-24 18:05:126</Data><Data Name='ProcessGuid'>{46C7284<!--Image--><System><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='Ipv6'>false</Data><Data Name='SourceIp'>192.168.250.20</Data><Data Name='SourcePortName'>microsoft-ds</Data><Data Name='DestinationHostname'></Data><Data Name='DestinationPort'>6406</Data><Data Name='Host'>we9041srv</Data><!--source-->source = WinEventLog:Microsoft-Windows-Sysmon/Operational

| stats count by src\_ip

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

| rename count as requests

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

Want to know more? Check out:

Splunk Quick Reference Guide: <https://splk.it/SplunkQuickRef>

Search manual: <https://splk.it/SplunkSearchManual>

# Working with statistics? Use **stats** and **functions**

## Usage

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

## Examples

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

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

Calculates statistics based on fields in your events

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



Creates a time series chart with a corresponding table of statistics

Want to know more? Check out:

Splunk Quick Reference Guide: <https://splk.it/SplunkQuickRef>

splunk>

# Stats Introduction

## Examples of stats



| stats count

*Returns the total number of events on 1 line*

| stats count by src\_ip

*Returns the total number of events per src\_ip*

| stats min(bytes) avg(bytes) max(bytes) by src\_ip

*Returns minimum, average & maximum bytes per src\_ip*

| stats dc(src\_ip) by dest\_ip

*Returns the number of (or distinct) src\_ips connecting to dest\_ip*

| stats avg(bytes) by \_time, src\_ip

*Returns average bytes per time slice and src\_ip*



# Indexing Basics

Where the Data Meets  
Controls

splunk>



# Indexing Basic Rules

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



# Sourcetype Basics

Where you define the  
format of your data!

splunk>

# Sourcetype Basics

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



# Sourcetype Basics

## Examples

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

Subject:

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

Process Information:

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

WinEventLog:Security

Multi Line Breaking  
Complex Field Extractions  
Process ID needs Hex Decoding

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

fortigate:utm

Single Line Breaking  
Key=Value pair Extractions





# Extracting Fields Basics

Where you make your  
data useable

splunk>

# Field Extraction Basics



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

# Field Extraction

## Chpt 2 - Search 1

### Extract a Field

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 v 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" ap msg="Network.Service: NTP," apprisk=elevated

**(.\*?)**

**Regular Expression**

Splunk Enterprise will extract fields using a Regular Expression.

**x|y|z**

**Delimiters**

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).

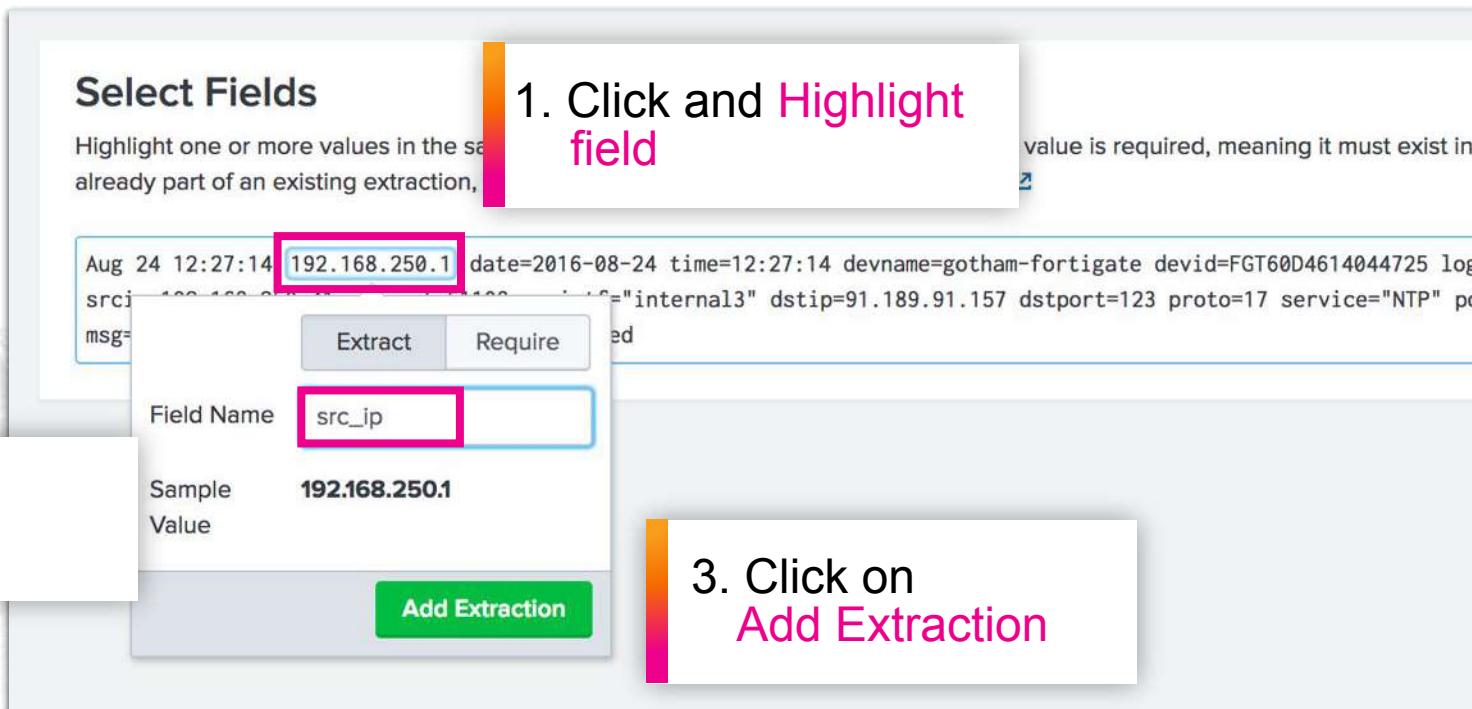
1. Click Regular Expression

2. Click on Next

# Field Extraction

## Chpt 2 - Search 1

### Highlight and Name



# Field Extraction

## Chpt 2 - Search 1

### Verify Field and Set Access

**Extract Fields**

Select Method → Select Fields → Validate → Save

**Next >**

**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 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=FGT6004614044725 1  
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"  
msg="Network.Service: NTP," apprisk=elevated

Show Regular Expression >

**Preview**

If you see incorrect results below, click an additional event to add it to the set of sample events. Highlight its values to improve the extraction. You can remove incorrect values in the Events list.

Events **src\_ip**

2. Click Next

**Extract Fields**

Select Method → Select Fields → Validate → Save

**Finish >**

**Save**

Name the extraction and set permissions.

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

Owner: admin

App: security\_4\_ropies

Permissions: App (selected)

	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
car_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"/>

4. Click Next

3. Set the Permissions



# Event Types & Tags Basics

Where you make  
correlated data scale

splunk>

# Event Types & Tags Basics

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



# 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

VPN Logon Success Event

vpn\_auth\_success

Windows Logon Failure Event

win\_auth\_failure

Linux Logon Failure Event

linux\_auth\_failure

VPN Logon Failure Event

vpn\_auth\_failure

Tag

authentication

failure

# Eventtypes and Tags

Chpt 3 - Search 1

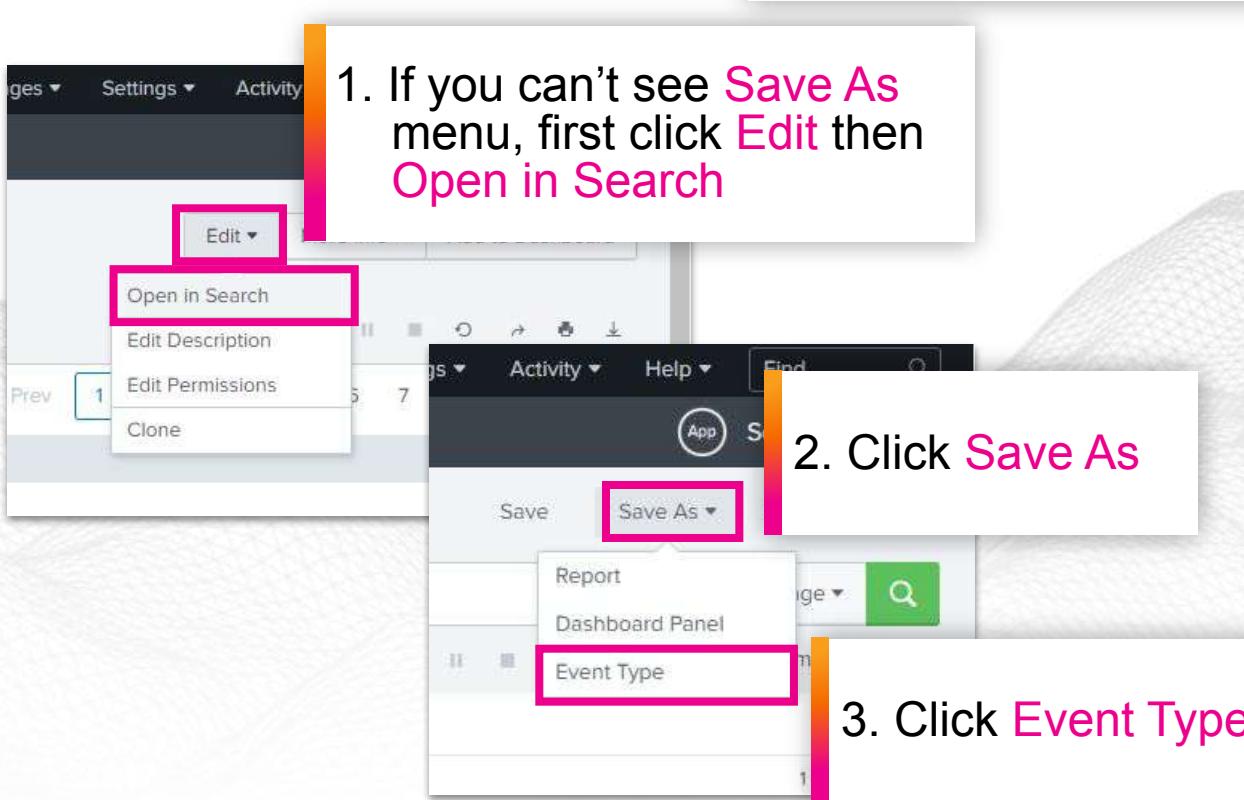
## Creating an eventtype

The screenshot shows the Splunk Enterprise search interface. The top navigation bar includes the 'splunk>enterprise' logo, the 'App: Security4Rookies' dropdown, and menu items for 'Search', 'Datasets', 'Reports', 'Alerts', 'Dashboards', and 'Results'. A search bar contains the query: `index="botsv1" sourcetype="WinEventLog:Security" (EventCode=4624)`. Below the search bar, the results summary indicates `3,209 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000)` and 'No Event Sampling'. The main pane displays the search results under the 'Events (3,209)' tab, with options for 'Format Timeline', 'Zoom Out', 'Zoom to Selection', and 'Deselect' at the bottom.

# Eventtypes and Tags

## Chpt 3 - Search 1

### Creating an eventtype



Name: **win\_auth\_success**  
Tags: **success, authentication**  
Priority: **1 (Highest)**

**Save As Event Type**

Name:	win_auth_success
Tags:	success, authentication
Color:	none ▾
Priority:	1 (Highest) ▾

Determines which style wins, when an event has more than one event type.

4. Click **Save**

# Eventtypes and Tags

## Chpt 3 - Search 2

### Searching by Tags

1. Enter  
**tag=authentication tag=success**

#### New Search

`tag=authentication tag=success`

✓ 3,209 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000)

Events (3,209)

Patterns

Statistics

Visualization

Format Timeline ▾

– Zoom Out

+ Zoom to Selection

2. Click **eventtype**

a Authentication\_Package 4  
a ComputerName 3  
# EventCode 1  
a eventtype 1  
# EventType 1  
a Impersonation\_Level 3  
a index 1  
# Key\_Length 2  
a Keywords 1  
# linecount 3  
a LogName 1  
a Logon\_GUID 29

### Searching by Tags

Time	Event
24/08/2016 19:27:24.000	08/24/2016 11:27:24 AM
	LogName=Security
	SourceName=Microsoft Windows security auditing.
	EventCode=4624
	EventType=0
	Show all 49 lines

eventtype

1 Value, 100% of events

Selected Yes No

#### Reports

Top values Top values by time

Rare values

Events with this field

#### Values

win\_auth\_success

3. Note that new  
**eventtype** is seen

# Bonus Material

## Chpt 3 - Search 3

### REGEX for the brave

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

- Search Bar:** Contains the search command:

```
| rex field=<field_name> "(?P<>)"  
| rex field=<field_name> "beforepattern(?P<extract_name>field_match)afterpattern"
```
- Navigation Bar:** Includes links for Search, Datasets, Reports, Alerts, Dashboards, and Ready Made Searches.
- New Search Panel:** Displays the search command and its results.
- Search Results:** Shows 413 events from 10/08/2016 to 24/08/2016. The event count is highlighted in blue.
- Event Details:** The first event is displayed with the full search command:

```
tag=authentication | rex field=form_data "username=(?P<user>.*?)&.*passwd=(?P<password>.*?)"
```
- Event Sampling:** Shows "No Event Sampling".
- Event Types:** Events (413), Patterns, Statistics, Visualization.
- Timeline Controls:** Format Timeline, Zoom Out, Zoom to Selection, Deselect.



# Break Time

15 min refuel

splunk>

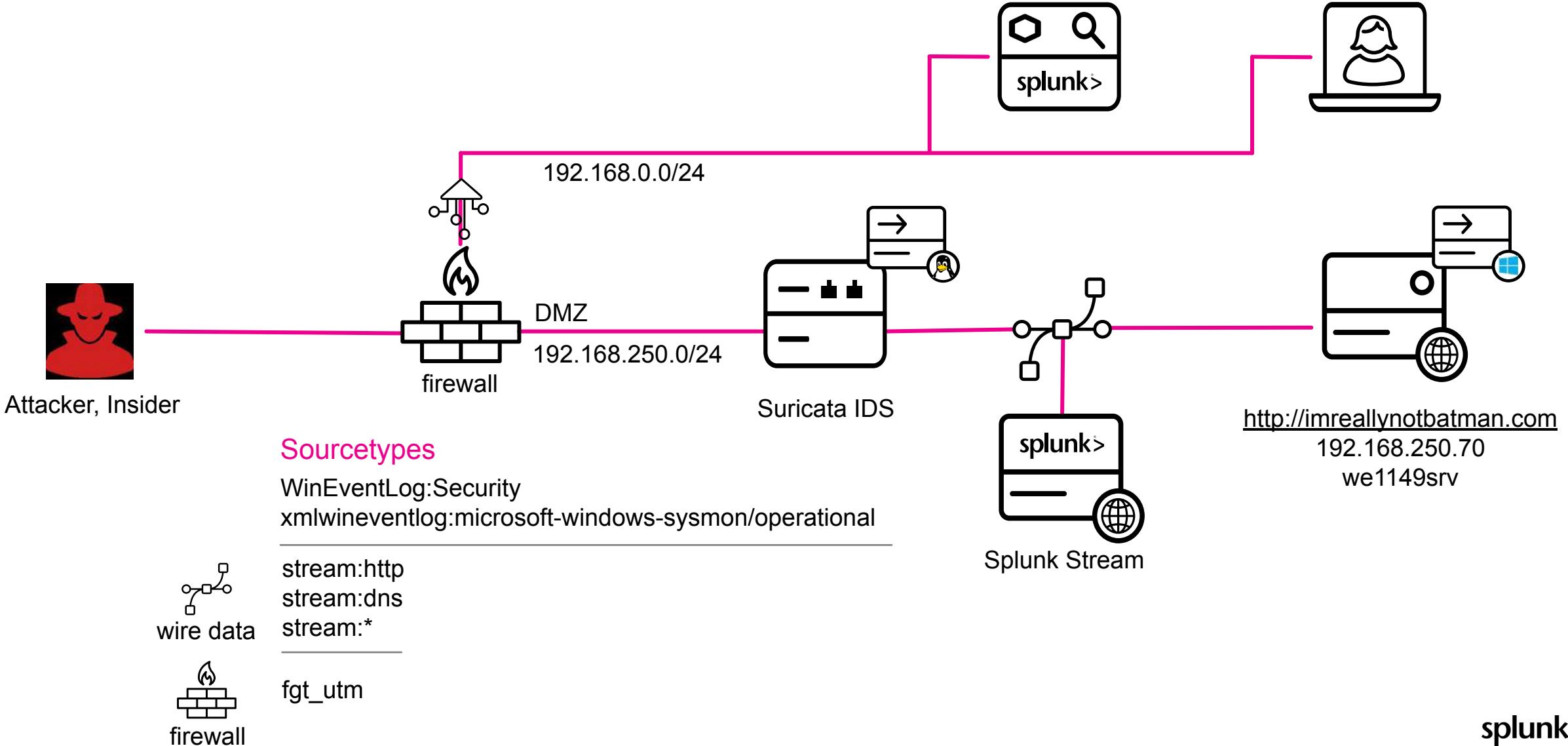
imreallynotbatman.com

# Security Data and Searches

For Security People



# WayneCorp Network



# Discovering the Attack

Chpt 4 - Search 1

## Filter Traffic to the Web Server

The screenshot shows the Splunk Enterprise search interface. The top navigation bar includes the 'splunk>enterprise' logo, the 'App: Security4Rookies' dropdown, and tabs for 'Search', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. A search bar contains the query: 'index="botsv1" sourcetype=stream:http dest\_ip=192.168.250.70'. A tooltip on the right side of the search bar displays the same query. Below the search bar, the results are shown: 'New Search' with a count of '20,275 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000)' and 'No Event' status. At the bottom, there are tabs for 'Events (20,275)', 'Patterns', 'Statistics', and 'Visualization'. The Splunk logo is in the bottom right corner.

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

✓ 20,275 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000) No Event

Events (20,275) Patterns Statistics Visualization

# Discovering the Attack

Chpt 4 - Search 2

Use stats to Aggregate

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

- Search Bar:** The search bar contains the command: `index="botsv1" sourcetype=stream:http dest_ip=192.168.250.70 | stats count(src_ip) BY src_ip`.
- Results Summary:** Below the search bar, it says "✓ 20,275 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000)" and "No Events".
- Statistics Tab:** The "Statistics (3)" tab is selected, indicated by a blue underline.
- Event List:** The event list shows two entries:
  - src\_ip = 192.168.2.50
  - src\_ip = 23.22.63.114
- Bottom Right Corner:** The Splunk logo "splunk>" is visible.

# Discovering the Attack

Chpt 4 - Search 3

## Rename Fields on the Fly

New Search

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

✓ 20,275 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000) No Event Sampling ▾

Events

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



# Discovering the Attack

## Chpt 4 - Search 4

### Using the sort Command

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

- Search Bar:** The search bar contains the command: `index="botsv1" sourcetype=stream:http dest_ip=192.168.250.70 | stats count(src_ip) AS requests BY src_ip | sort - requests`.
- Statistics Panel:** The Statistics tab is selected, showing three results:

src_ip	requests
40.80.148.42	17546
23.22.63.114	1429
23.22.63.114	214
- Annotations:**
  - A pink circle highlights the IP address `40.80.148.42` in the results table, with a magnifying glass icon pointing to it.
  - A pink box highlights the value `17546` in the `requests` column of the results table.
  - A text box with a pink background and orange gradient border contains the text: "Optional ‘-’ to sort order".
  - A text box with a pink background and orange gradient border contains the text: "Sorted results".

# Discovering the Attack

Chpt 4 - Search 5

## Investigate the Source Headers

Chpt4 - Search 5

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

✓ 20,275 events | 10/08/2016 03:22

Events (20,275) Patterns

Format Timeline ▾ Zoom

1. Delete from | stats onwards

A screenshot of a Splunk search interface titled "Chpt4 - Search 5". The search bar contains the query "1 index='botsv1' sourcetype=stream:http dest\_ip=192.168.250.70". Below the search bar, it says "✓ 20,275 events | 10/08/2016 03:22". There are two tabs: "Events (20,275)" and "Patterns". A color scale from green to red is shown next to the tabs. Below the tabs, there are filters for "Format", "Timeline", and "Zoom". A large pink magnifying glass highlights the "src\_headers" field in a list of event fields. A hand cursor is pointing at the "src\_headers" field. A callout bubble says "1. Delete from | stats onwards".

Time	Event
> 24/08/2016	{ [-] 162742405 }

2. Scroll down and click src\_headers

c\_ip: 1  
cached:  
cancel:  
capture:

image/jpeg, image/png, \*/\*

```
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=v7ikb3m59rbiet3vhv3 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: \*/\*

3. Note Acunetix Web Vulnerability Scanner

A screenshot of a Splunk search results page. The top part shows a single event with the following details: "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=v7ikb3m59rbiet3vhv3", "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", and "Accept: \*/\*". A large pink rectangle highlights the "Acunetix-Scanning-agreement" and "Acunetix-User-agreement" lines. A callout bubble says "3. Note Acunetix Web Vulnerability Scanner".

# Discovering the Attack

Chpt 4 - Search 6

## Investigate the Traffic

Chpt4 - Search 6

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

✓ 20275 events (10/08/2016 03:28:51.000 to 24/08/2016 18:27:44.000) No Event Sampling ▾ Job ▾ II III ▾ Smart Mode ▾

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

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

# Discovering the Attack

# Chpt 4 - Search 7

# Investigate Data Being Received

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 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&sea
&ordering=!((()&!|*|*)&searchphrase=all&sea
&ordering=!((()&!|*|*)&searchphrase=any&sea
&ordering=!((()&!|*|*)&searchphrase=exact&s
&ordering=!((()&!|*|*)&searchphrase=exact&s
&ordering="+response.write(9006556*9070592)
```

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

1. Page through acunetix web scanning things!

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

# Discovering the Attack

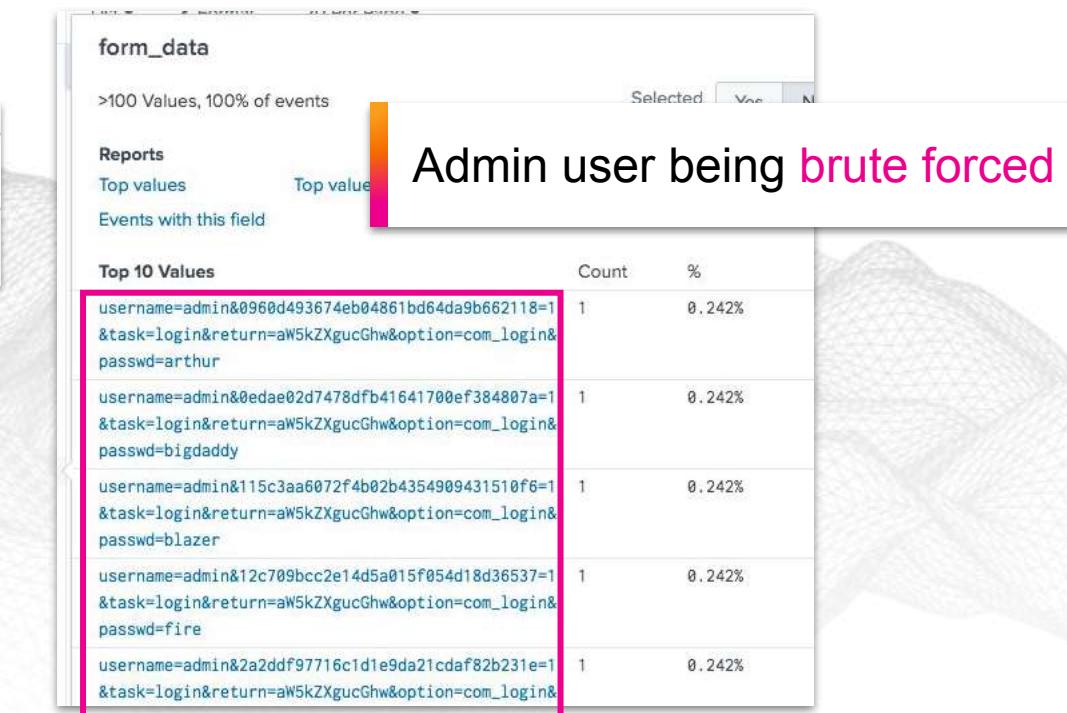
Chpt 4 - Search 8

## Investigate Login Activity

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

✓ 413 events (10/08/2016 03:28:51.000 to 24/08/2016 18:27:44.000) No Event Sampling ▾

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



# Discovering the Attack

## Chpt 4 - Search 9

### Inspect the login activity

The screenshot shows a Splunk search interface. On the left, a sidebar lists various event fields such as dest\_headers, dest\_ip, dest\_mac, dest\_port, duplicate\_packets\_in, duplicate\_packets\_out, endtime, eventtype, form\_data, http\_comment, http\_content\_length, index, linecount, location, missing\_packets\_in, missing\_packets\_out, and network\_interface. The 'form\_data' field is highlighted with a red box and labeled '1. Click form\_data'. On the right, a detailed view of the 'form\_data' search results is shown. The top section shows filters: dest\_port: 80 and duplicate\_packets\_in: 1. Below this, under 'Reports', are 'Top values' and 'Events with this field'. Under 'Values', there is a table with one row: 'username=admin&passwd=batman&option=com\_login&task=login&return=aW5kZXgucGhw&e5ec827a3f67ce0efc546d81f7356acc=1' with a count of 1 and 100% probability. A pink bar highlights this row. To the right of the table, the text '2. Successful login' is displayed. At the bottom of the right panel, there is a list of other event fields: packets\_out: 5, reply\_time: 1672760, request: POST /joomla/administrator/index.php HTTP/1.1, request\_ack\_time: 51724, and request\_time: 0.

dest\_headers 1  
dest\_ip 1  
dest\_mac 1  
dest\_port 1  
duplicate\_packets\_in 1  
duplicate\_packets\_out 1  
endtime 1  
eventtype 1  
form\_data 1  
http\_comment 1  
http\_content\_length 1  
index 1  
linecount 1  
location 1  
missing\_packets\_in 1  
missing\_packets\_out 1  
network\_interface 1

dest\_port: 80  
duplicate\_packets\_in: 1

**form\_data**

1 Value, 100% of events

Selected Yes No

**Reports**

Top values

Events with this field

Values

username=admin&passwd=batman&option=com\_login&task=login&return=aW5kZXgucGhw&e5ec827a3f67ce0efc546d81f7356acc=1

Count %

packets\_out: 5  
reply\_time: 1672760  
request: POST /joomla/administrator/index.php HTTP/1.1  
request\_ack\_time: 51724  
request\_time: 0

1. Click **form\_data**

2. Successful login



# Unauthorized Access

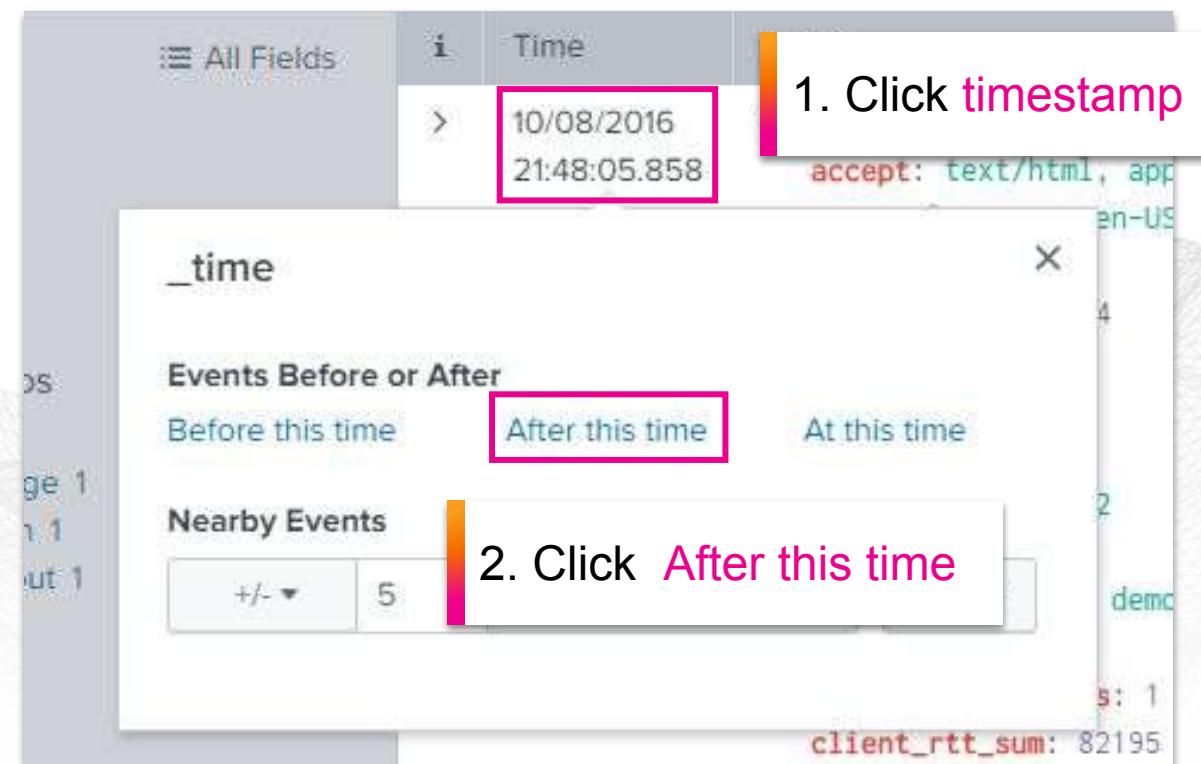
What happened next

splunk>

# Post Exploit

Scene Setting

## Set the time range



# Post Exploit

## Chpt 5 - Search 1

### Looking for a Dropper File

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

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

	i	Time	Event
>	10/08/2016 22:52:47.035	{"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": "57", "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, "host": "192.168.250.70", "http_method": "POST", "http_status": 200, "http_version": "HTTP/1.1", "log_level": "INFO", "source": "botnet", "src_ip": "192.168.250.70", "src_mac": "00:0C:29:C4:02:7E", "type": "http"}, "raw": "HTTP/1.1 200 OK\r\nContent-Type: text/html; charset=UTF-8\r\nContent-Length: 57\r\n\r\nhis program cannot be run in DOS mode.\r\n\r\n", "type": "http"} <td>Executable uploaded</td>	Executable uploaded

# Post Exploit

## Chpt 5 - Search 2

### Investigate Endpoint Process

#### 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 ▾

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

# Post Exploit

## Chpt 5 - Search 2

### Investigate Endpoint Process

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

imnotbatman.jpg Overwritten!

# Post Exploit

## Chpt 5 - Search 3

### Investigate Web Server Activity

#### 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 ▾

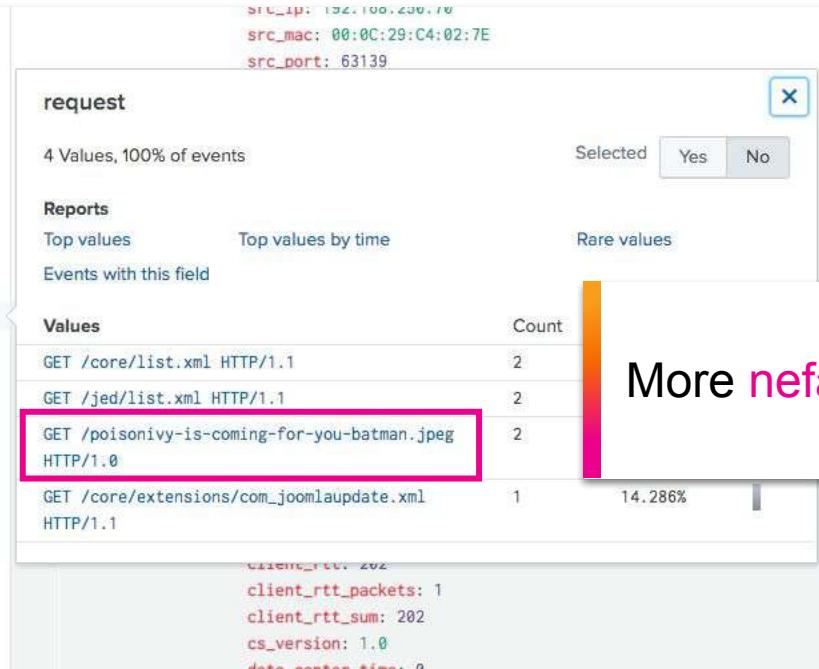
```
index="botsv1"  
sourcetype=stream:http  
http_method="POST"  
src_ip=192.168.250.70
```

# Post Exploit

## Chpt 5 - Search 3

### Investigate Web Server Activity

```
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  
a sc_cache_control 1  
a sc_date 2  
a server 1  
# server_rtt 7  
# server_rtt_packets 2  
# server_rtt_sum 7  
a site 2  
a splunk_server 1  
a src_headers 4
```



More nefarious behaviour

# Post Exploit

## Chpt 5 - Search 3

### Investigate Web Server Activity

#### 1. Fetching the jpeg

```
g_packets_out: 0
k_interface: eth1
s_in: 6
s_out: 5
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
```

#### 2. DDNS Site



# Dashboards

My Manager wants  
them now! - OK

splunk>

# Dashboards

## Chpt 6 - Search 1

### Brute Force Activity

2. Click Save As, then Dashboard Panel

splunk>enterprise App: Security4Rookies

Administrator 2 Messages

Search Datasets Reports Alerts Dashboards Network Diagram Ready Made Searches

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 / APPPOOL\DefaultAppPool	IIS / APPPOOL\joomla	NT / AUTHORITY\IUSR	NT / AUTHORITY\LOCAL SERVICE	NT / AUTHORITY\NETWORK SERVICE	NT / AUTHORITY\SYSTEM	WAYNECORPINC\Administrator	WAYNECORPINC\bob.smith	Window Manager\DWManager	admin	NULL
splunk-02											

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

# Dashboards

## Chpt 6 - Search 1

1. Click New

### Brute Force Activity

Save As Dashboard Panel

Dashboard  New  Existing

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

**Dashboard Title:** Security Operations  
**Dashboard ID:** security\_operations  
**Dashboard Desc:** My First Dashboard  
**Panel Title:** Password attempts per user

splunk>

# Dashboards

Chpt 6 - Search 2

## Unexpected Logon Sources

Chpt6 - Search 2

```
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 ▾

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

# Dashboards

## Chpt 6 - Search 2

### Unexpected Logon Sources

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

Cluster Map Format Trellis

1. Select Cluster Map, under Visualization

latitude longitude

39.04738 -77.47449

185.10.200.26

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

Save As

Date time range ▾

Save As ▾ View Close

Verbose Mode ▾

Dashboard New Existing

Panel Title Security Operations ▾

Panel Powered By  Inline Search  Report

Drilldown? No action

Panel Content  Statistics  Cluster Map

Cancel Save

splunk>

# Dashboards

## Chpt 6 - Search 3

### Analyse Useragent Lengths

#### 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 ▾

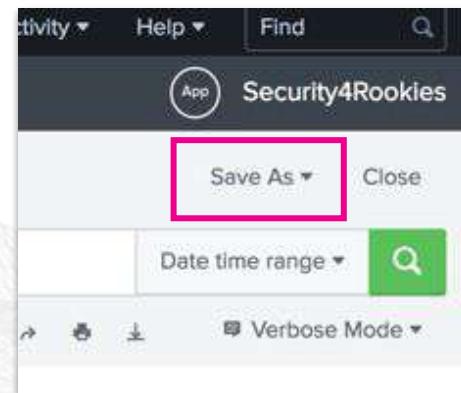
Join

```
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
```

# Dashboards

## Chpt 6 - Search 3

### Analyse Useragent Lengths



Save As Dashboard Panel

Dashboard	New	Existing
Security Operations ▾		
Panel Title	[Empty input field]	
Panel Powered By	Inline Search	Report
Drilldown	No action	
Panel Content	Statistics	Cluster Map
<input type="button" value="Cancel"/> <input type="button" value="Save"/>		

# Dashboards

Chpt 6 - Search 4

## Analyse Web Traffic

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

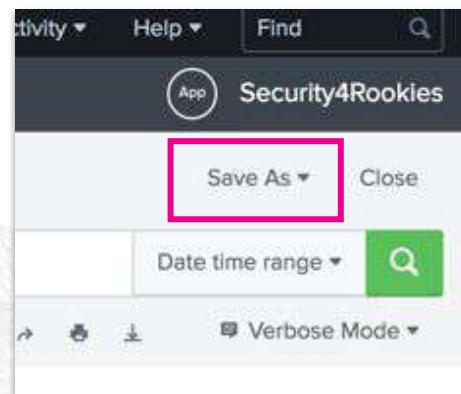
✓ 20,061 events (10/08/2016 20:00:00.000 to 10/08/2016 22:59:59.000) No Event Sampling ▾

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

# Dashboards

## Chpt 6 - Search 4

### Analyse Web Traffic



A screenshot of the 'Save As Dashboard Panel' dialog box. It has tabs for 'New' and 'Existing', with 'Existing' highlighted by a red box. Below that is a dropdown menu set to 'Security Operations'. The 'Panel Title' field is also highlighted by a red box. Underneath, there are sections for 'Panel Powered By' (with 'Inline Search' selected), 'Drilldown' (set to 'No action'), and 'Panel Content' (with 'Statistics' selected). At the bottom right are 'Cancel' and 'Save' buttons, with 'Save' highlighted by a red box.

# Dashboards

## Chpt 6 - Search 5

### Web Logins by External IP

#### New Search

```
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
```

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

```
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

## Chpt 6 - Search 5

### Web Logins by External IP

The screenshot shows the Splunk interface for creating a search. A color bar on the left transitions from green to red. The main area displays a search results table with 413 events from August 8, 2016, to August 24, 2016. The 'Visualization' tab is selected. A modal window titled '42 Single Value' is open, showing the configuration for a single value visualization. The 'Format' tab is selected in the modal. The 'Color' section uses a red-to-green gradient. A legend on the right indicates 'Green for 0' and 'Red for > 0'. The 'Ranges' section shows five color-coded ranges: 0-30 (blue), 30-70 (yellow), 70-100 (orange), 100-max (red), and a green range for 0 (green). The 'Color Mode' section shows two radio buttons labeled '42' and '42' with a green background.

1. Select Visualization

2. Select Single Value

3. Select Format

Green for 0  
Red for > 0

42 Single Value ✓ Format

General Use Colors

Color Color by

Number Format

Ranges from min to 0

from 0 to 30

from 30 to 70

from 70 to 100

from 100 to max

+ Add Range

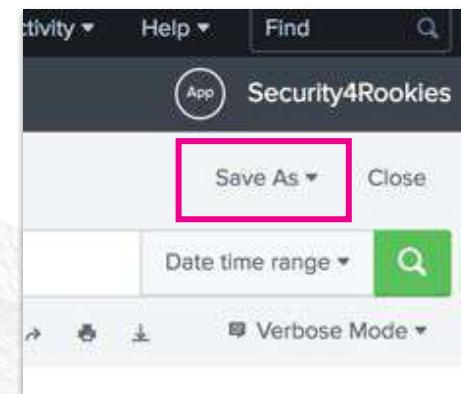
Color Mode 42 42

2016-08-19

# Dashboards

## Chpt 6 - Search 5

### Web Logins by External IP



Save As Dashboard Panel

Dashboard	New	Existing
Security Operations		
Panel Title		
Panel Powered By	Inline Search	Report
Drilldown	No action	
Panel Content	Statistics	Cluster Map
<button>Cancel</button> <button>Save</button>		

# Dashboards

Chpt 6 - Search 6

## Scanning Activity

### 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 ▾

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

# Dashboards

## Chpt 6 - Search 6

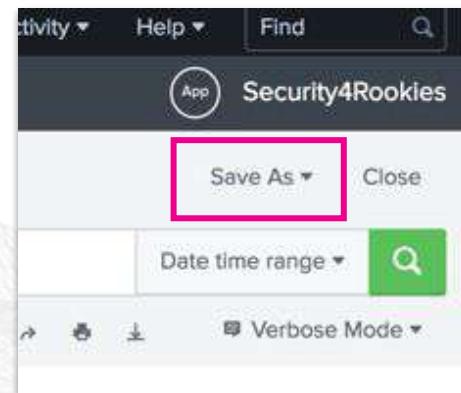
### Scanning Activity

The image shows a composite screenshot of the Splunk interface. On the left, a 'New Search' bar contains the query `index="botsv1" sourcetype=stream: 016 04:28:51.0`. Below it, a navigation bar includes 'Events (13,394)', 'Patterns', 'Statistics (79)', and a highlighted 'Visualization' tab. A callout box labeled '1. Select Visualization' points to the 'Visualization' tab. Another callout box labeled '2. Select Single Value' points to a button in the search bar labeled '42 Single Value'. A third callout box labeled '3. Select Format' points to a button in the search bar labeled 'Format'. On the right, a detailed view of the 'Visualization' tab shows settings for a 'Single Value' visualization. It includes options for 'Use Colors' (set to 'Yes'), 'Color by' ('Value' selected), and color ranges from green to red. A note at the bottom states 'Green for 0 Red for > 0'.

# Dashboards

## Chpt 6 - Search 6

### Scanning Activity



A screenshot of the 'Save As Dashboard Panel' dialog box. It has tabs for 'New' and 'Existing', with 'Existing' selected and highlighted by a red box. Below that is a dropdown menu set to 'Security Operations'. The 'Panel Title' field is empty and highlighted by a red box. Under 'Panel Powered By', there are options for 'Inline Search' (selected) and 'Report'. The 'Drilldown' section shows 'No action'. The 'Panel Content' section has two options: 'Statistics' (selected) and 'Cluster Map'. At the bottom are 'Cancel' and 'Save' buttons, with 'Save' highlighted by a red box.

# Dashboards

## Select Dashboard

The screenshot shows the Splunk Enterprise search interface. At the top, there's a navigation bar with tabs: Search, Datasets, Reports, Alerts, Dashboards, Network Diagram, and Ready M. The 'Dashboards' tab is highlighted with a pink box. Below the navigation bar is a search bar labeled 'Search' with a placeholder 'enter search here...'. Underneath the search bar is a dropdown menu for 'No Event Sampling'. A callout box with a pink border and the text '1. Select Dashboards' points to the 'Dashboards' tab in the navigation bar.

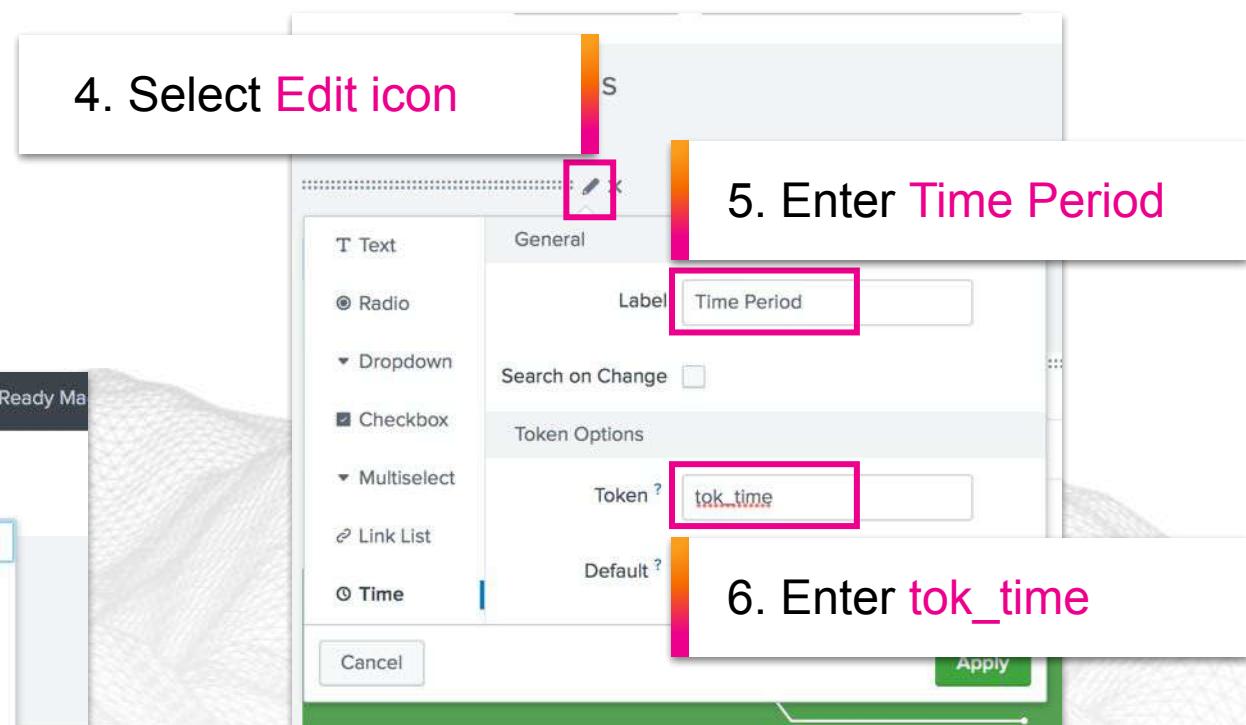
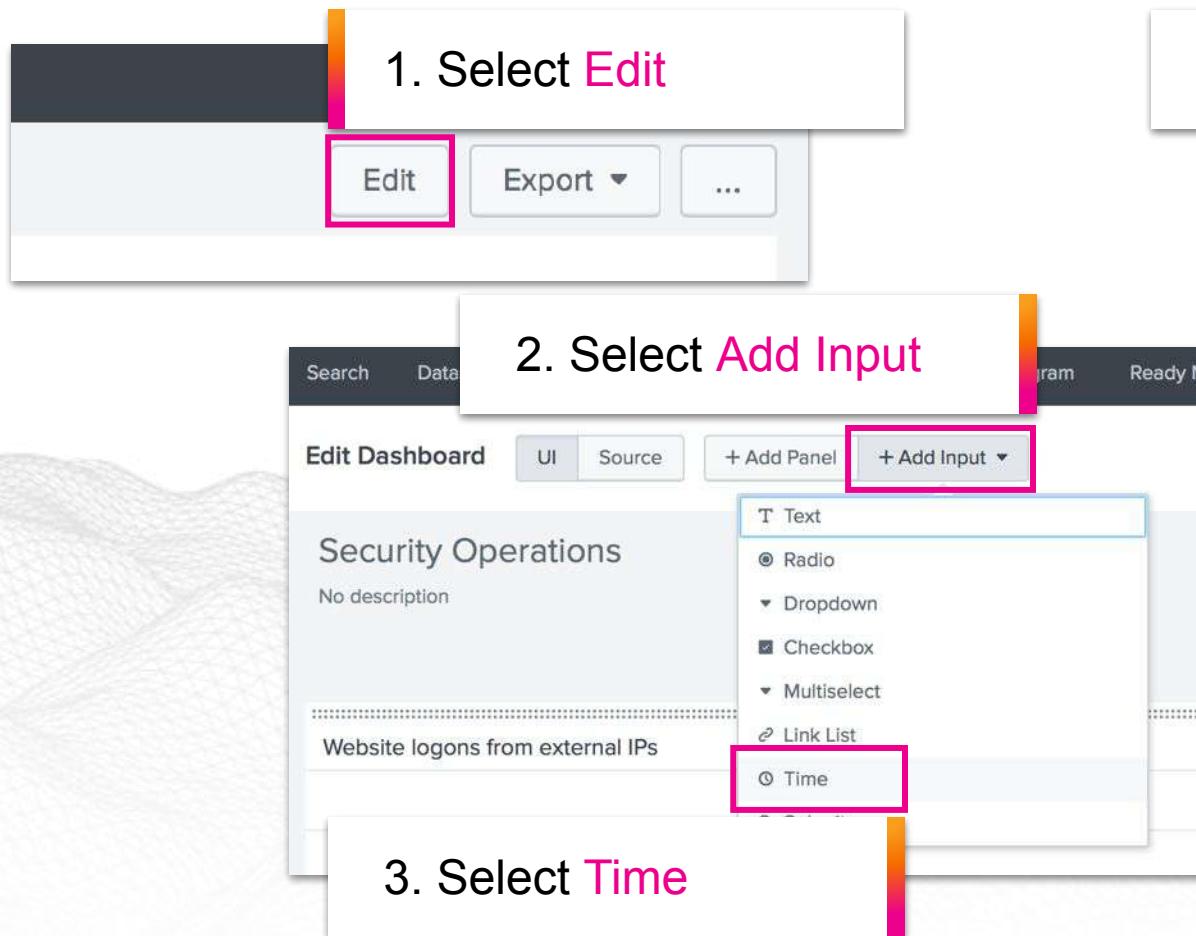
This screenshot shows a list of dashboards. The title 'Dashboards' is at the top. Below it, it says 'Dashboards include searches, visualizations, and in...' and '2 Dashboards'. There are two items in the list: 'Network Diagram' and 'Security Operations'. The 'Security Operations' item is highlighted with a pink box. A callout box with a pink border and the text '2. Select Security Operations' points to the 'Security Operations' item in the list.

This screenshot shows the 'Security Operations' dashboard. At the top, there's a navigation bar with tabs: Search, Datasets, Reports, Alerts, Dashboards, Network Diagram, Ready Made Searches, and a user icon with 'Security4Rookies'. Below the navigation bar is a section titled 'Password attempts per user' with a table. The table has columns for 'host' (with value 'splunk-02') and 'user' (with value 'admin'). On the right side of this section is an 'Edit' button, which is highlighted with a pink box. A callout box with a pink border and the text '3. Select Edit' points to the 'Edit' button.

splunk>

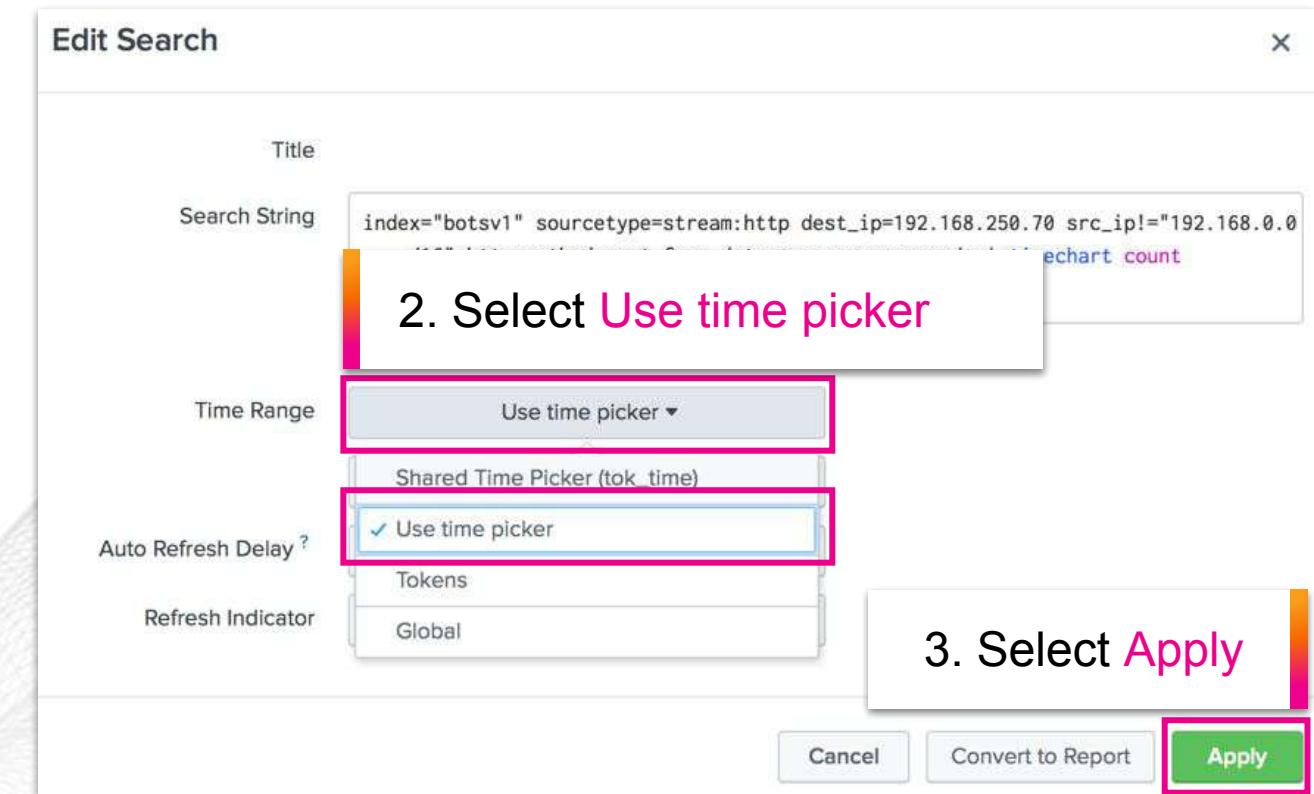
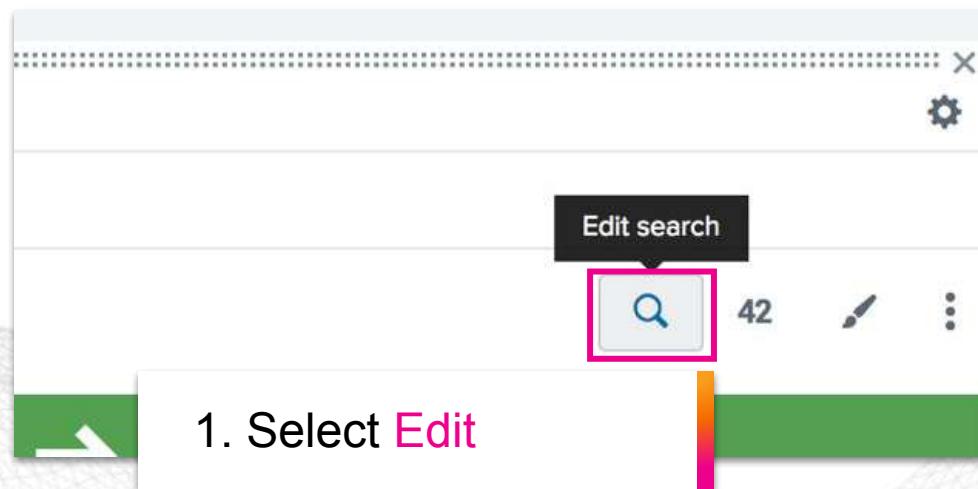
# Dashboards

## Add Input



# Dashboards

## Use Token



# Dashboards

## Change Visualisation

1. Select Visualization Type

host	IIS APPPOOL\DefaultAppPool	IIS APPPOOL\joomla	NT AUTHORITY\USR	NT AUTHORITY\LOCAL SERVICE	NT AUTHORITY\NETWORK SERVICE	NT AUTHORITY\SYSTEM	WAYNECORPINC\Administrator	WAYNECORPINC\bob.smith	Window Manager\DWL-3
we1149srv	1	1	1	1	1	1	0	0	1
we8105desk	0	0	0	1	1	1	1	1	0
we9041srv	0	0	0	1	1	1	1	0	1

2. Select Column Chart

SPLUNK VISUALIZATIONS

- Bar
- Line
- Area
- Scatter
- Map
- 42
- Column Chart
- Donut
- Dot
- Geo Dot
- Gauge
- Table
- Text
- Image
- World Map
- Region Map

Find more visualizations [↗](#)

Column Chart

3. Select Edit

General

Stack Mode

- all
- stacked 100%

Multi-series

Show

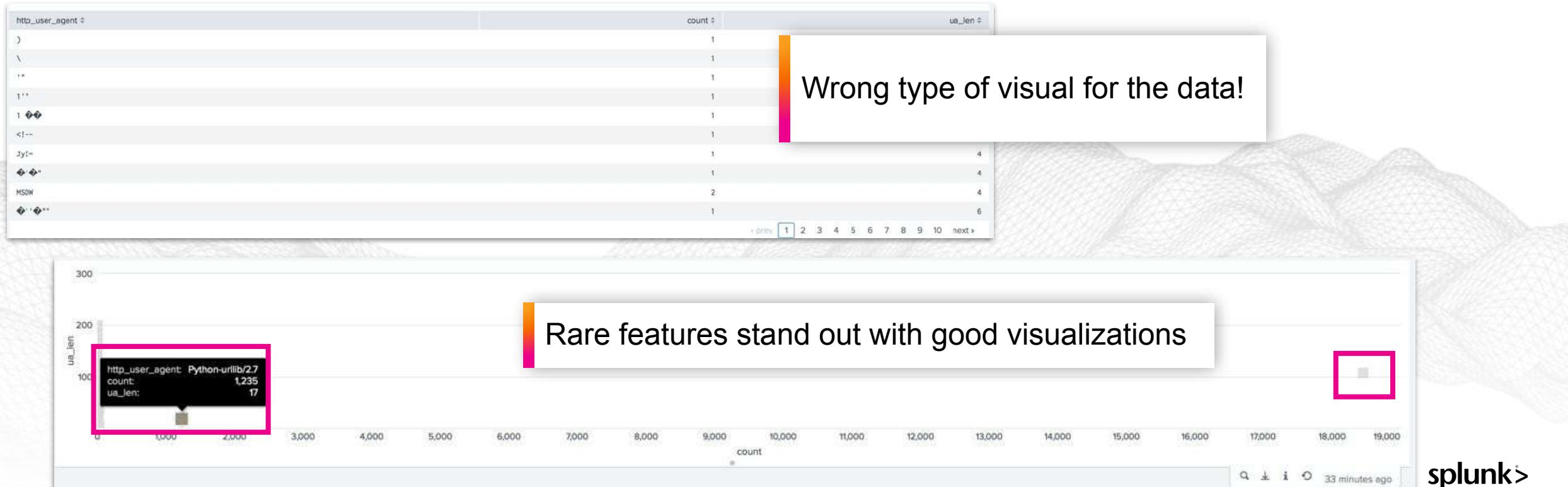
Legend

4. Select Stacked 100%

# Dashboards

## Visualizations

**Bonus Challenge: Change http\_user\_agent panel to a scatter chart**



# Dashboards

## Visualizations

### Interactive Filtering

1. Click Add Input

2. Select Dropdown

3. Enter user

4. Enter tok\_user

5. Click Apply

6. Scroll down

splunk>

# Dashboards

## Visualizations

### Interactive Filtering

Static Options

Name	Value
ALL	*

+ Add New

1. Enter ALL for Name and \* for Value

Dynamic Options

Content Type

Search String

Run Search [Run Search](#)

Last 24 hours

Field For Label ?

Field For Value ?

**Apply**

2. Enter | inputlookup user\_list | sort user

3. Enter user

4. Enter user

# Dashboards

## Visualizations

### Interactive Filtering

Token Options

Token ?

Default ?

Clear Selection

Initial Value ?

Clear Selection

Token Prefix ?

1. Select ALL

2. Select ALL

3. Scroll back up

T Text      General

Radio      Token Options

Dropdown      Static Options

Checkbox      + Add New

Multiselect      Dynamic Options

Link List      Content Type

Time      Search String

Last 24 hours

Field For Label ?

Field For Value ?

4. Click Apply

splunk>

# Dashboards

## Visualizations

### Substitute tokens into a dashboard search



Title

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
```

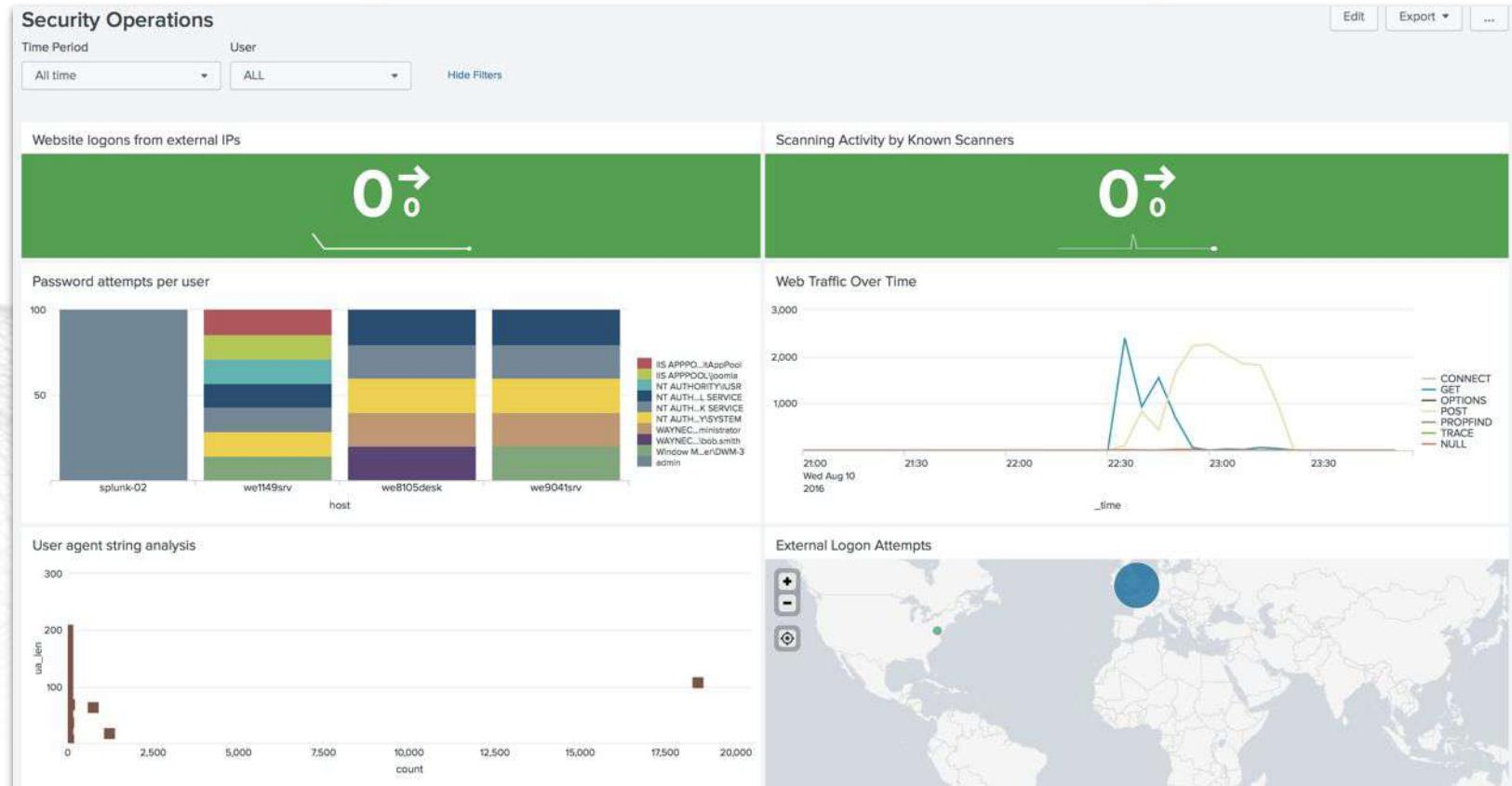
Run Search ↗

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

# Dashboards

## Visualizations

### Dashboard Complete





# Splunk Resources

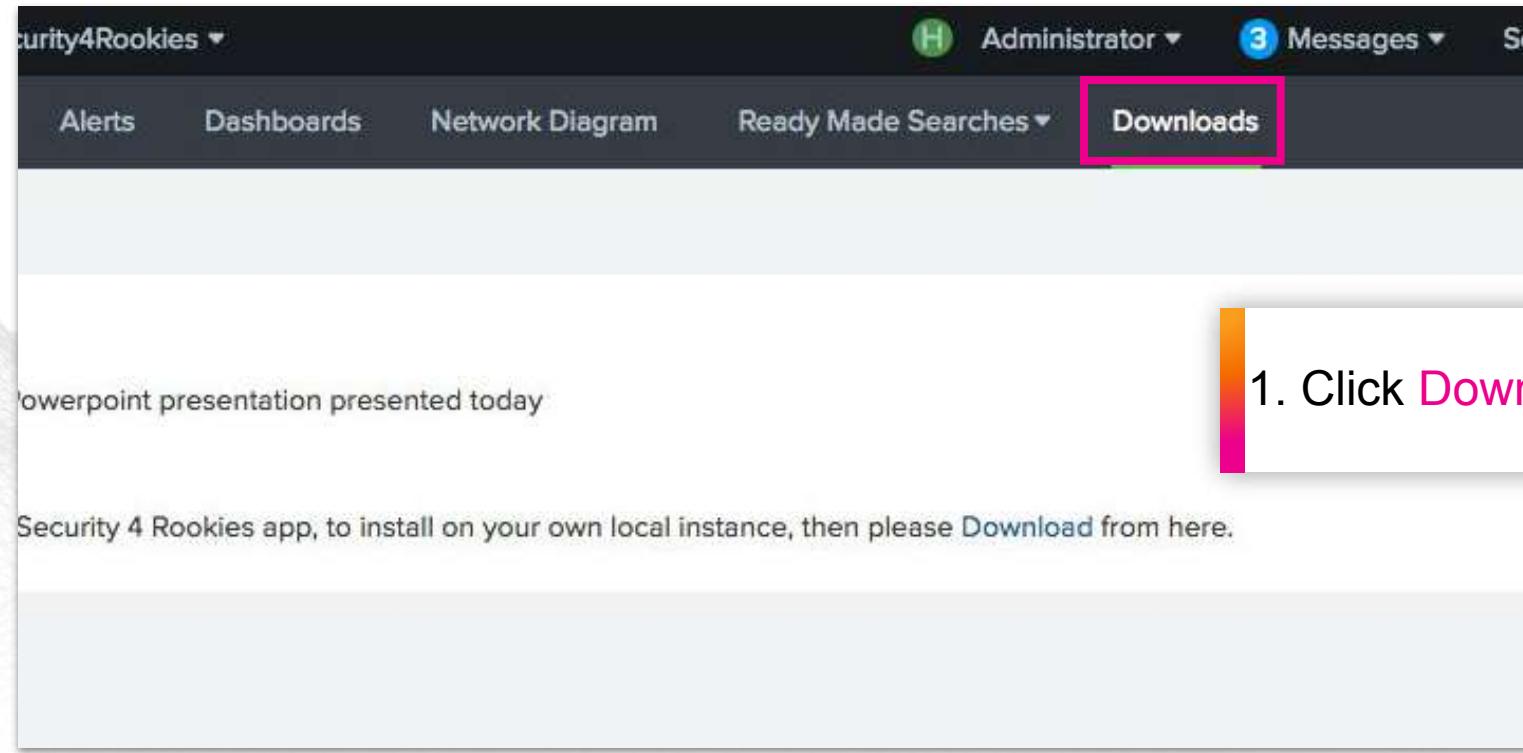
Where to go after  
today's workshop

splunk>

# Dashboards

## Visualizations

### Dashboard Complete



1. Click Downloads

[Register](#)

# Need more inspiration?

Security Dataset Project

**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!

**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>

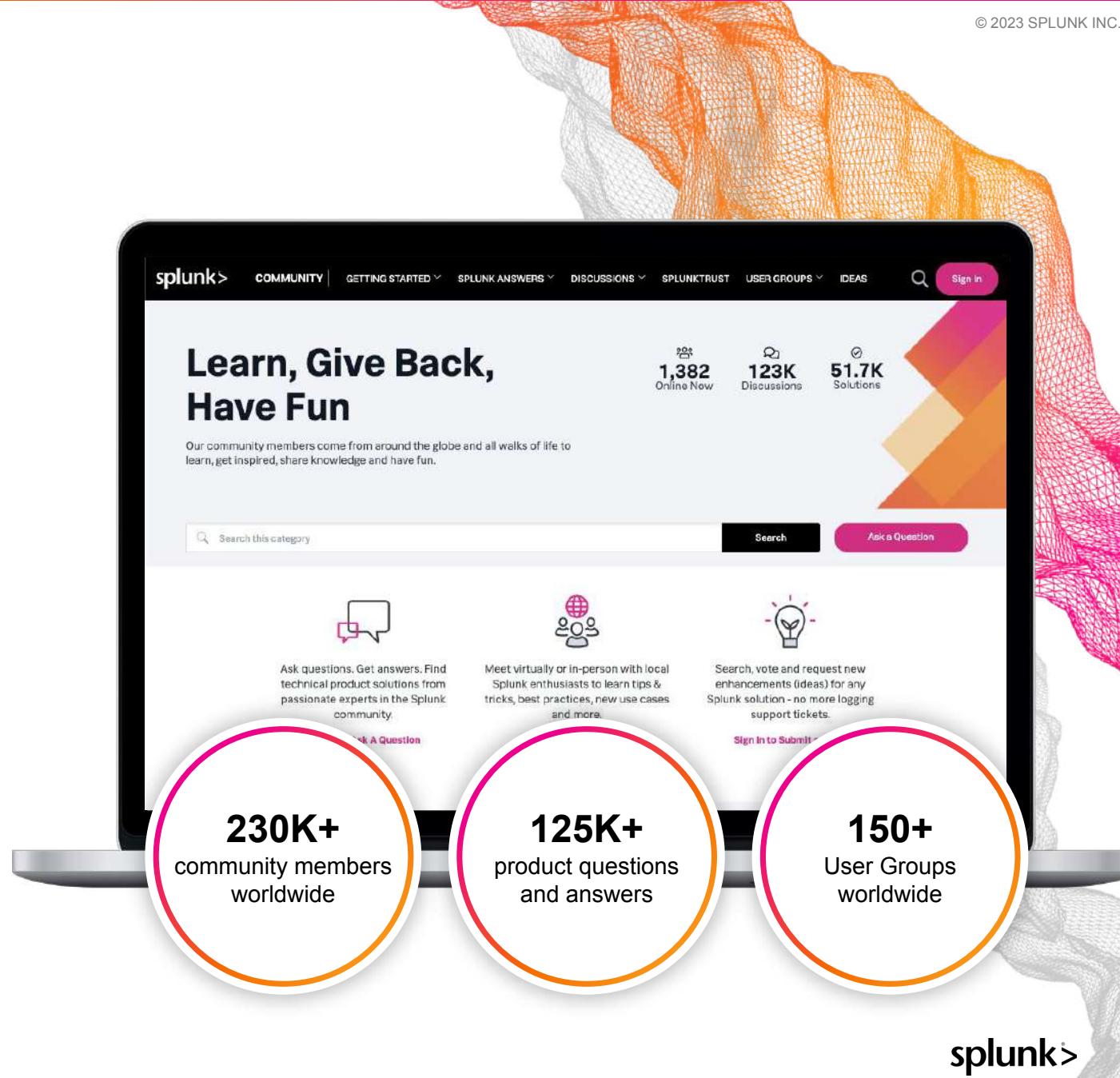


**splunk>**

# Splunk Community

<https://community.splunk.com>

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



# Splunk Events

<https://events.splunk.com>

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



<https://conf.splunk.com>

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

# Documentation

<https://docs.splunk.com>

- Search reference for SPL

- Step-by-step tutorials

Search

<https://splk.it/SplunkSearchTutorial>

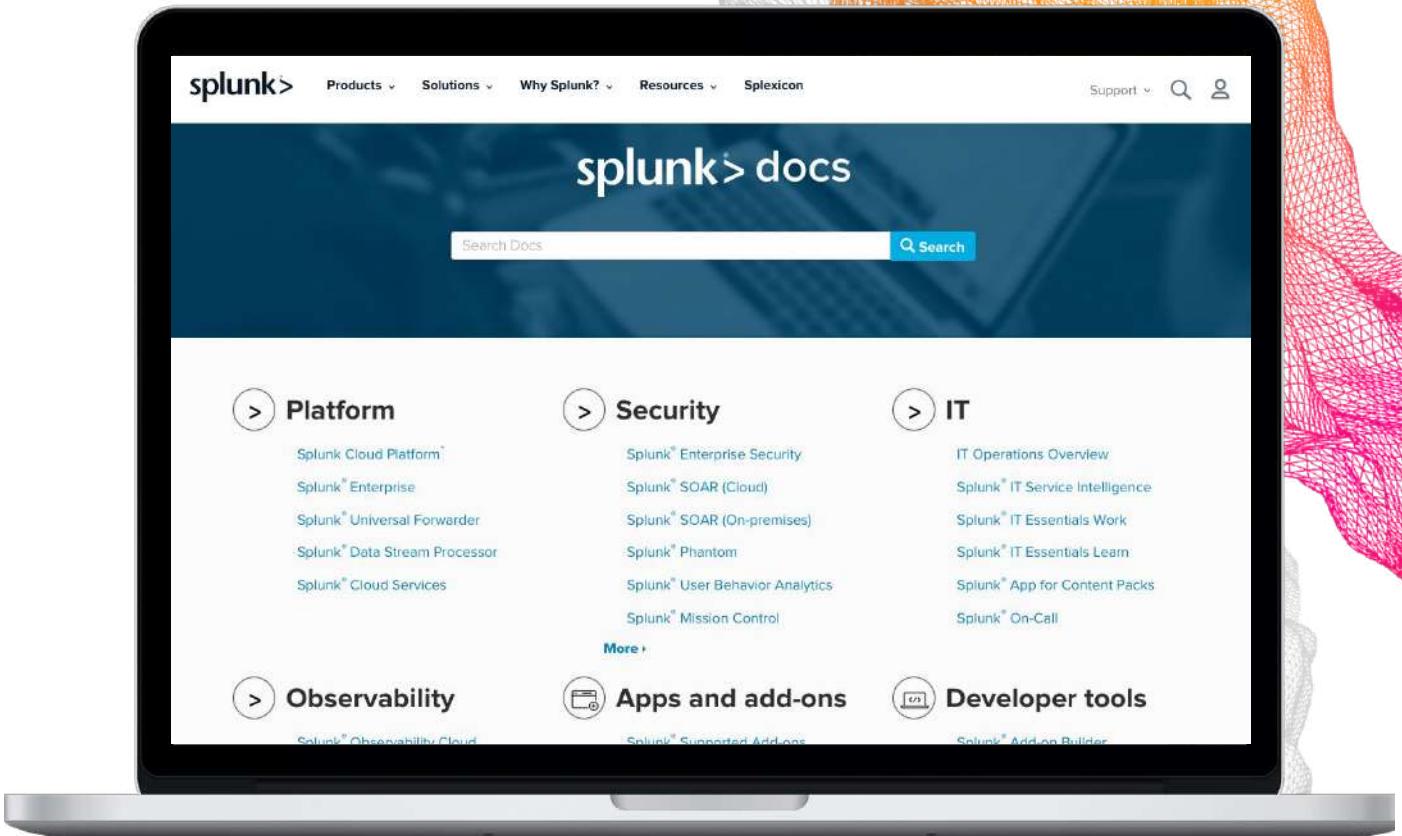
Dashboard Studio

<https://splk.it/SplunkDashStudioTutorial>

- Product references

- Procedures/guides

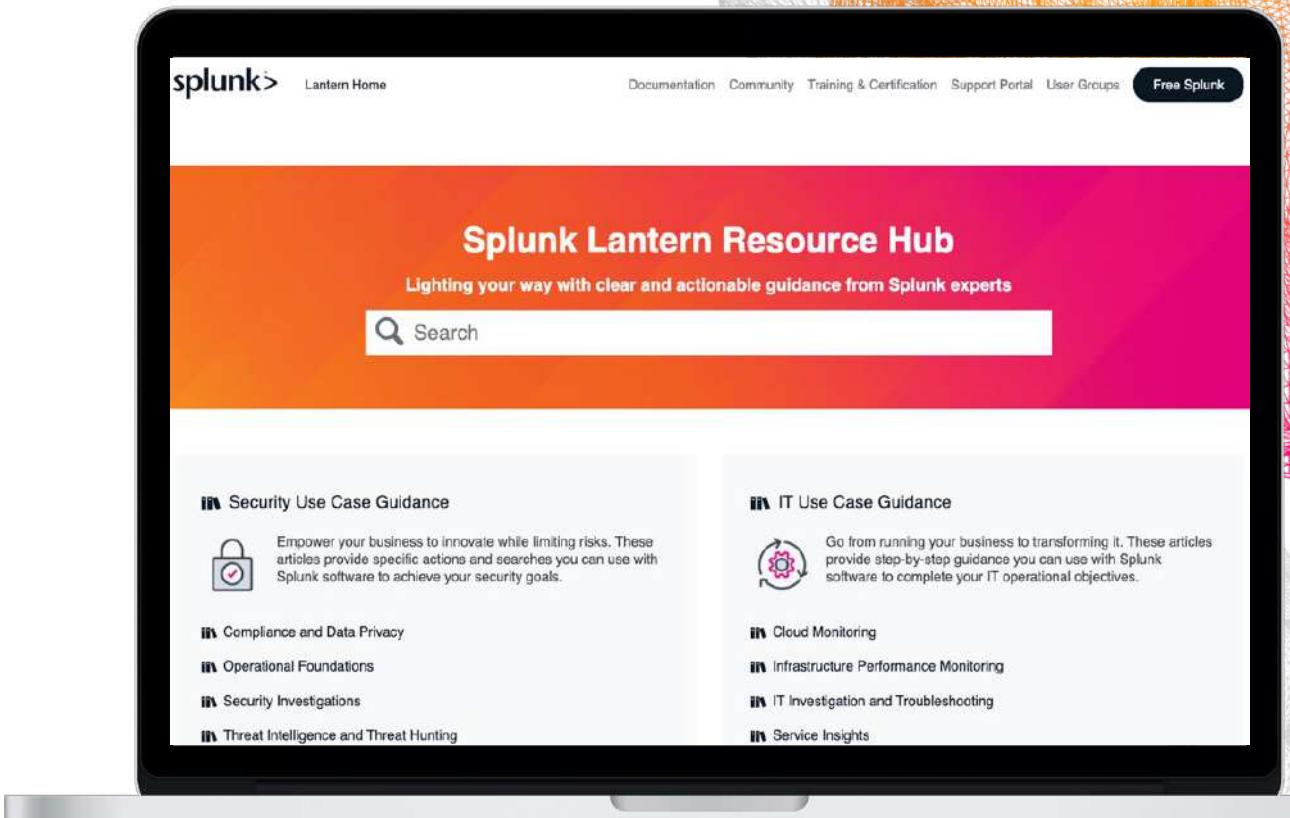
- And more!



# Splunk Lantern

<https://lantern.splunk.com>

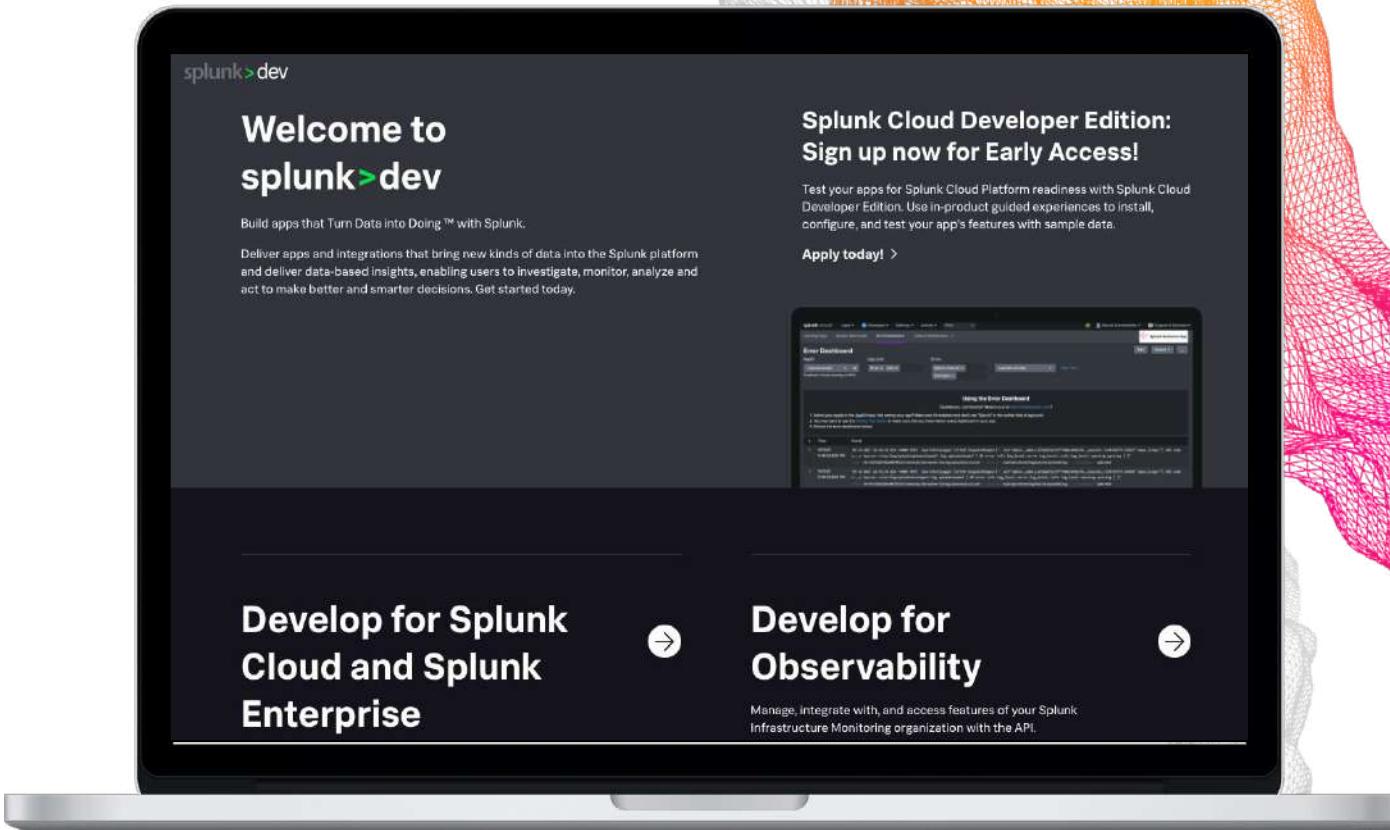
- Use case library
- Step-by-step procedures
- Map use cases to data sources
- Splunk Success Framework to realize value across your organisation



# Developer Resources

<https://dev.splunk.com>

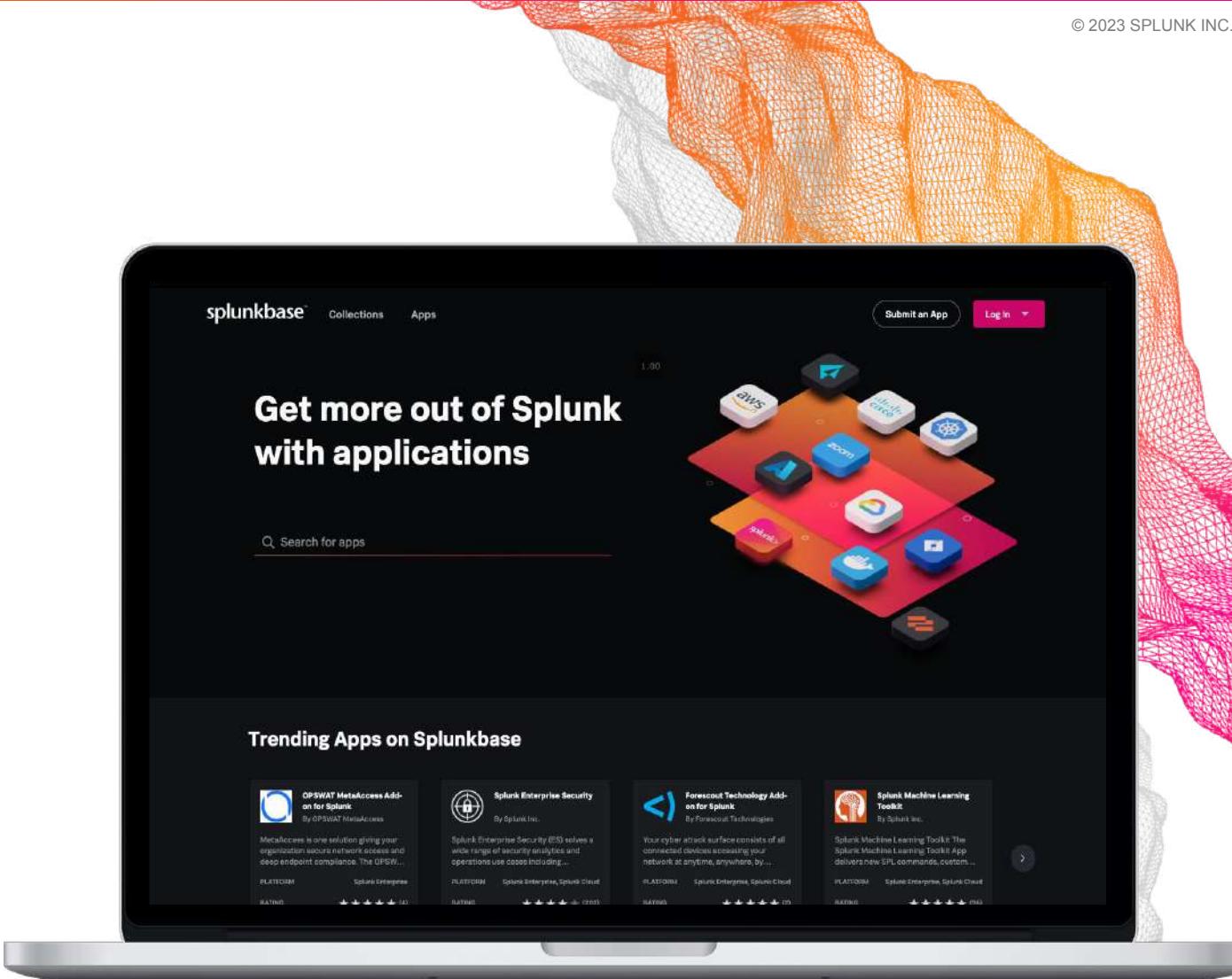
- Developer Guide
- API Reference
- Tutorials
- Downloads  
APIs, libraries, tools
- Code examples
- Free Developer licence
- Splunk Cloud Developer Edition  
Test your apps for Splunk Cloud readiness



# Splunk Apps & Add-ons

<https://splunkbase.splunk.com/>

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



# Training & Certification

<https://splunk.com/training>

Online education classes

Instructor-led and self-paced eLearning

Certification tracks for different roles

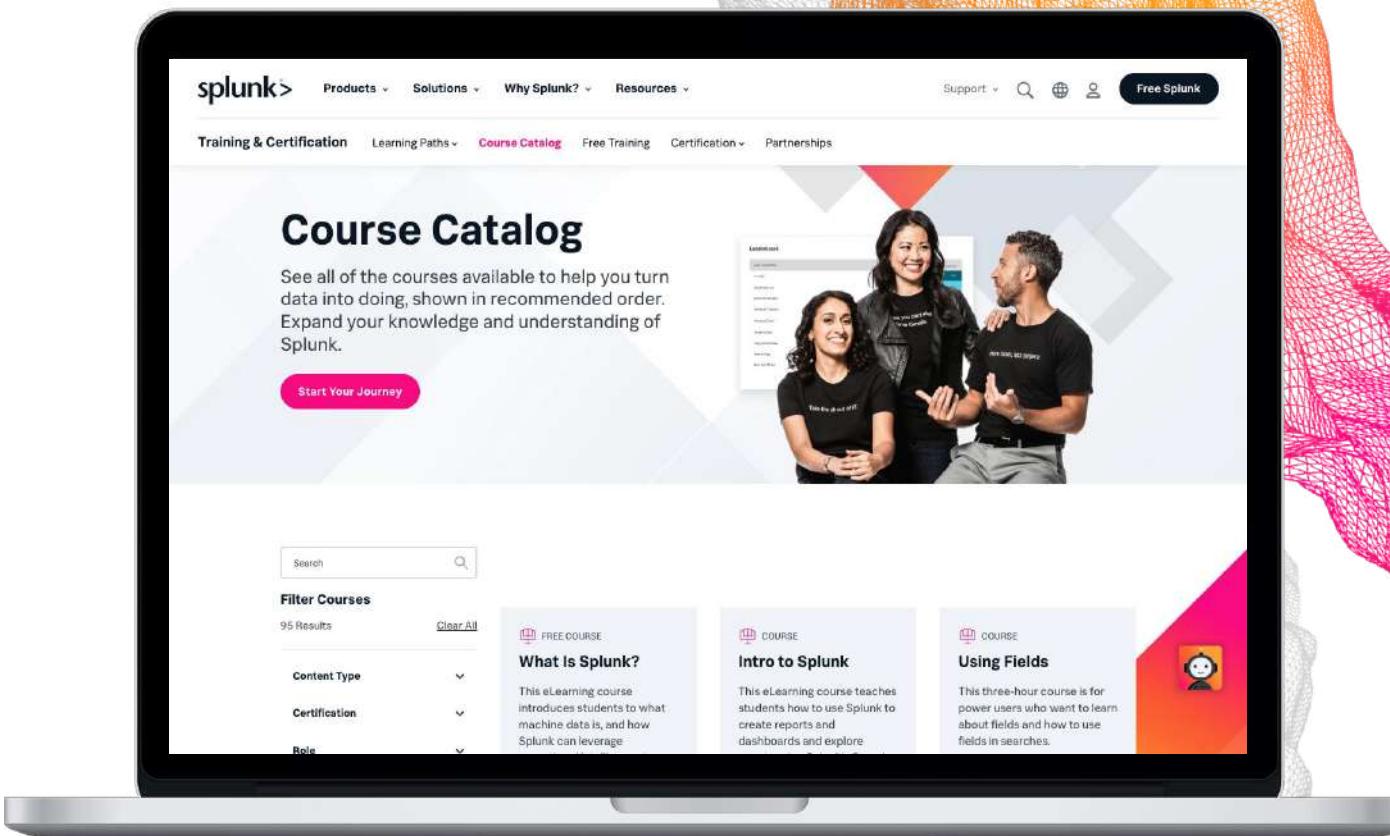
User, Power User, Admin, Architect and Developer

Splunk Education Rewards

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

Free education!

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



# Splunk for Security

Unifying data, analytics, and operations

## SPLUNK MISSION CONTROL

Splunk  
SIEM  
(ES & UBA)

Splunk  
SOAR  
(Phantom)

Splunk  
Security Apps  
(SSE & InfoSec)

Future Splunk  
Solutions &  
3<sup>rd</sup>-Party  
Tools

splunk®

Data Sources  
Logs, Business Context,  
Threat Intelligence

# Thank You!

