

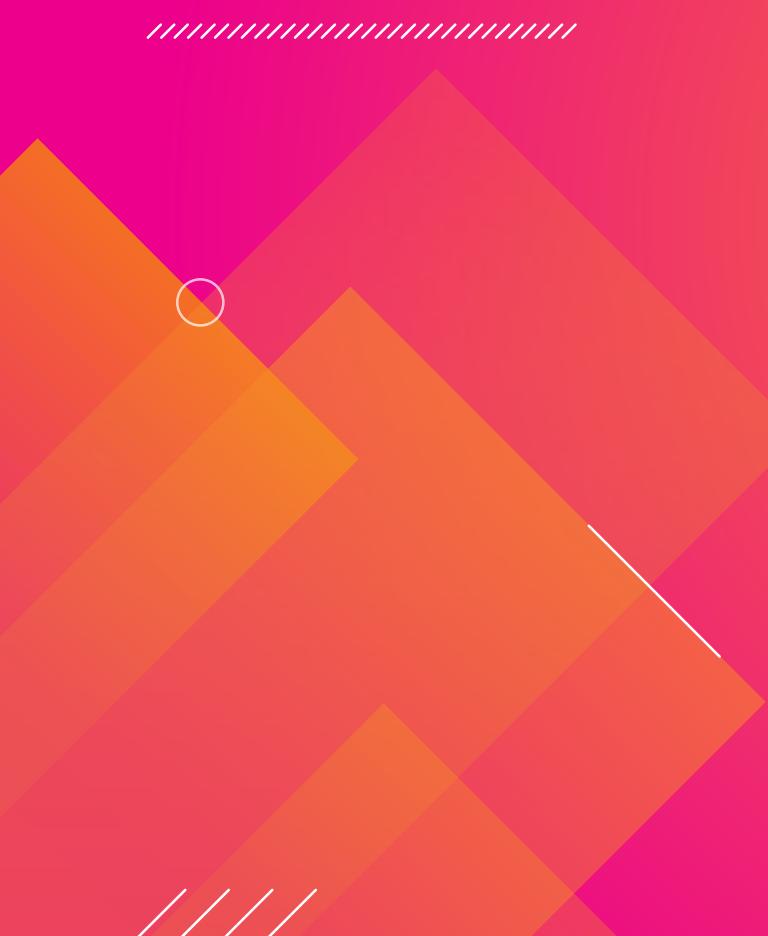
Splunk Security 4 Rookies



#Splunk4Rookies

splunk> turn data into doing™

Forward-Looking Statements



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

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

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

Agenda for Today's Workshop



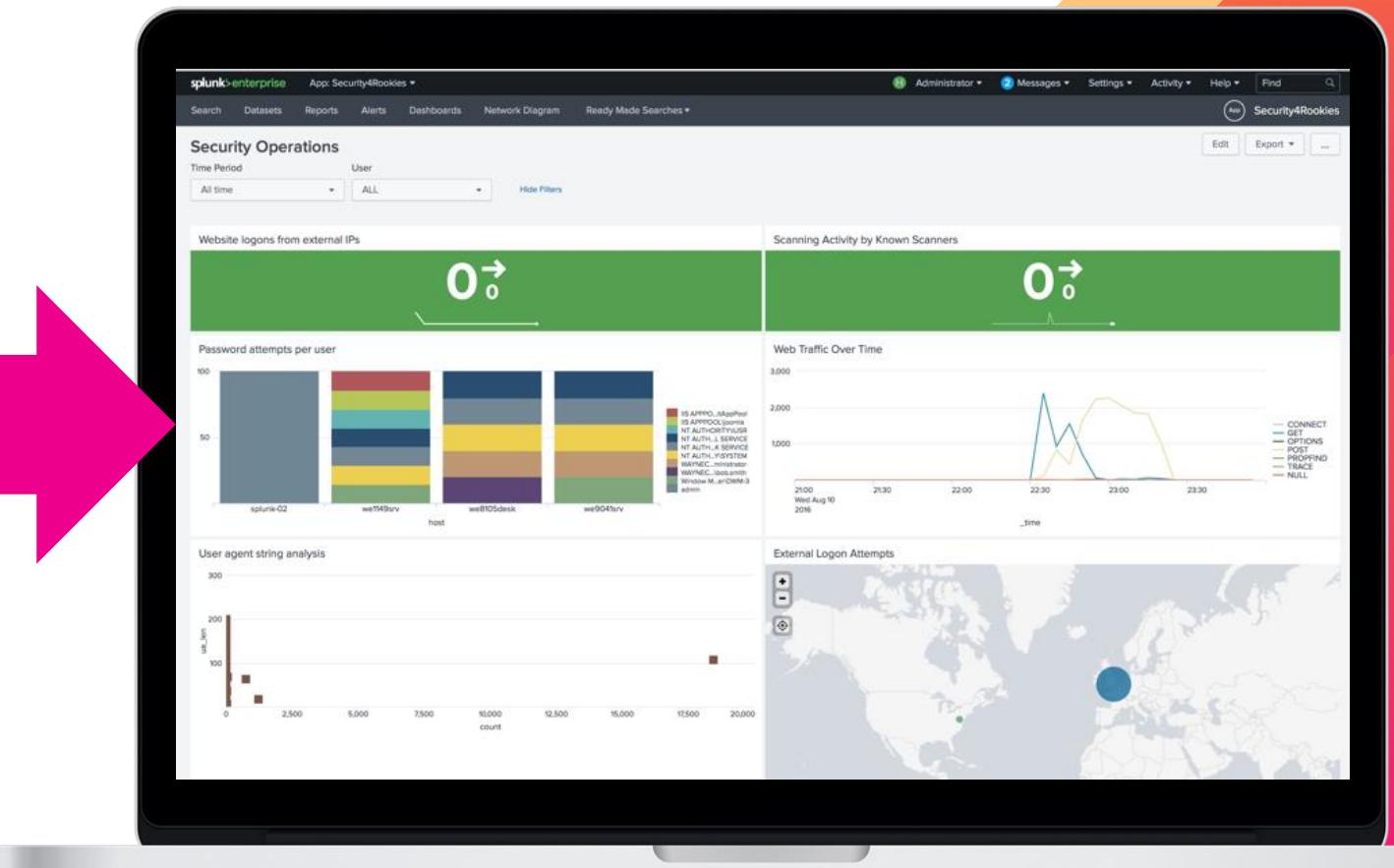
- ✓ Brief Splunk overview
- ✓ Search basics
- ✓ Indexing data
- ✓ Defining the format of your data
- ✓ Making data useable
- ✓ Aggregating and correlating data
- ✓ Put it into practice on web defacement investigation
- ✓ Creating proactive searches and dashboards

There's a Lot More to Splunk...

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

Objective

```
9.167.143.32 - - [01/Nov/2016 20:48:22:143] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL1FF4ADFF3 H  
TP 1.1" 200 1429 "http://www.myflowershop.com/cart.do?action=remove&itemId=EST-13&product_id=AV-CB-01" "Googlebot  
/2.1 ( http://www.googlebot.com/bot.html )" 403  
194.215.205.19 - - [01/Nov/2016 20:48:24:159] "GET /cart.do?action=changequantity&itemId=EST-7&product_id=FI-FW-02  
&JSESSIONID=SD1SL2FF9ADFF9 HTTP 1.1" 503 3699 "http://www.myflowershop.com/category.screen?category_id=FLOWERS" "M  
ozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 301  
130.253.37.97 - - [01/Nov/2016 20:48:24:198] "GET /cart.do?action=purchase&itemId=EST-27&product_id=RP-SN-01&JSESS  
IONID=SD3SL8FF4ADFF8 HTTP 1.1" 200 3350 "http://www.myflowershop.com/category.screen?category_id=SURPRISE" "Mozill  
a/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 927  
92.1.170.135 - - [01/Nov/2016 20:48:25:142] "GET /category.screen?category_id=TEDDY&JSESSIONID=SD0SL1FF10ADFF5 HTT  
P 1.1" 200 2906 "http://www.myflowershop.com/category.screen?category_id=TEDDY" "Mozilla/5.0 (Windows; U; Windows  
NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6" 967  
27.181.0.0 - - [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/9.0 (Windows NT 5.1; U; e  
n)" 389  
125.17.14.100 - - [01/Nov/2016 20:48:26:174] "GET /product.screen?product_id=AV-CB-01&JSESSIONID=SD0SL10FF4ADFF2 H  
TP 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=SD0SL1  
HTTP 1.1" 200 2438 "http://www.myflowershop.com/cart.do?action=view&itemId=EST-18&product_id=FL-DLH-02" "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=K9  
&JSESSIONID=SD0SL1FF9ADFF7 HTTP 1.1" 404 664 "http://www.myflowershop.com/product.screen?product_id=K9-BD-01  
bot/2.1 ( http://www.googlebot.com/bot.html )" 387  
94.229.0.21 - - [01/Nov/2016 20:48:31:177] "GET /category.screen?category_id=BOUQUETS&JSESSIONID=SD0SL7FF  
HTTP 1.1" 200 3770 "http://www.myflowershop.com/category.screen?category_id=BOUQUETS" "Mozilla/5.0 (Windows  
NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6" 814  
12.130.60.5 - - [01/Nov/2016 20:48:32:150] "GET /product.screen?product_id=AV-CB-01&JSESSIONID=SD1SL4FF5ADFF6 HTTP  
1.1" 200 2676 "http://www.myflowershop.com/category.screen?category_id=TEDDY" "Mozilla/4.0 (compatible; MSIE 6.0;  
Windows NT 5.1)" 177  
130.253.37.97 - - [01/Nov/2016 20:48:33:155] "GET /cart.do?action=addtocart&itemId=EST-1&product_id=AV-CB-01&JSESS  
IONID=SD10SL9FFF9ADFF7 HTTP 1.1" 200 933 "http://www.myflowershop.com/product.screen?product_id=AV-CB-01" "Googlebo  
t/2.1 ( http://www.googlebot.com/bot.html )" 493  
130.253.37.97 - - [01/Nov/2016 20:48:35:178] "GET /product.screen?product_id=AV-SB-02&JSESSIONID=SD08SL3FF6ADFF10 H  
TP 1.1" 200 3491 "http://www.myflowershop.com/cart.do?action=addtocart&itemId=EST-6&product_id=AV-SB-02" "Googleb  
ot/2.1 ( http://www.googlebot.com/bot.html )" 778  
131.178.233.243 - - [01/Nov/2016 20:48:35:188] "POST /product.screen?product_id=FI-FW-02&JSESSIONID=SD02SL2FF7ADFF2  
HTTP 1.1" 200 1023 "http://www.myflowershop.com/product.screen?product_id=FI-FW-02" "Mozilla/5.0 (Macintosh; U; I  
ntel Mac OS X 10.6.3; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 Safari/533.4" 936  
131.178.233.243 - - [01/Nov/2016 20:48:35:172] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD08SL4FF9ADFF2  
HTTP 1.1" 404 3679 "http://www.myflowershop.com/product.screen?product_id=FL-DSH-01" "Mozilla/4.0 (compatible; MS  
IE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 402  
141.146.8.66 - - [01/Nov/2016 20:48:37:141] "GET /product.screen?product_id=K9-BD-01&JSESSIONID=SD10SL8FF9ADFF8 HT  
TP 1.1" 200 1452 "http://www.myflowershop.com/category.screen?category_id=TEDDY" "Mozilla/4.0 (compatible; MSIE 6.  
0; Windows NT 5.1)" 118
```



Task 1: Register and Create Your Environment

Tasks:

1. Register:

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):

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

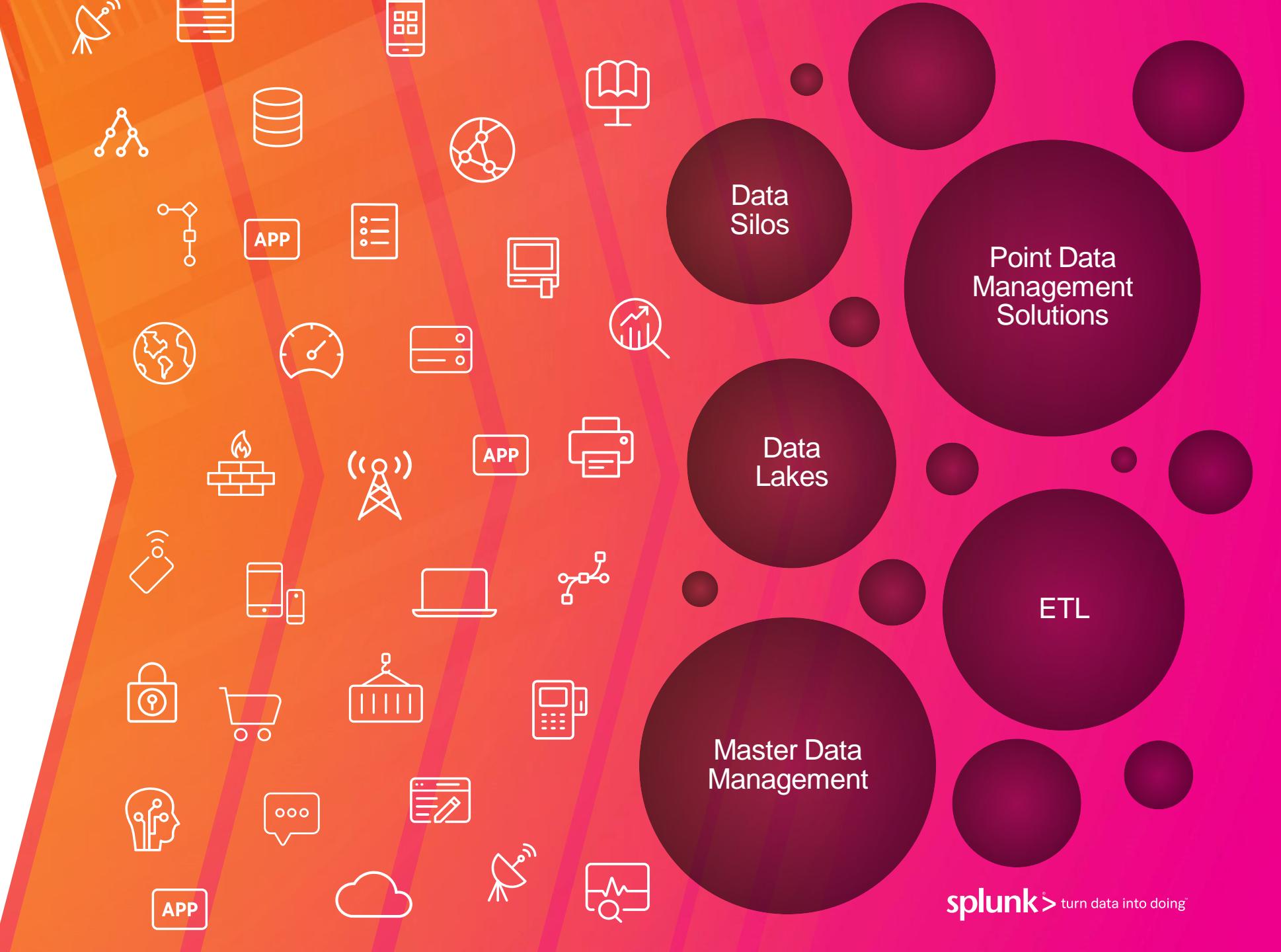
New
Technology

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**

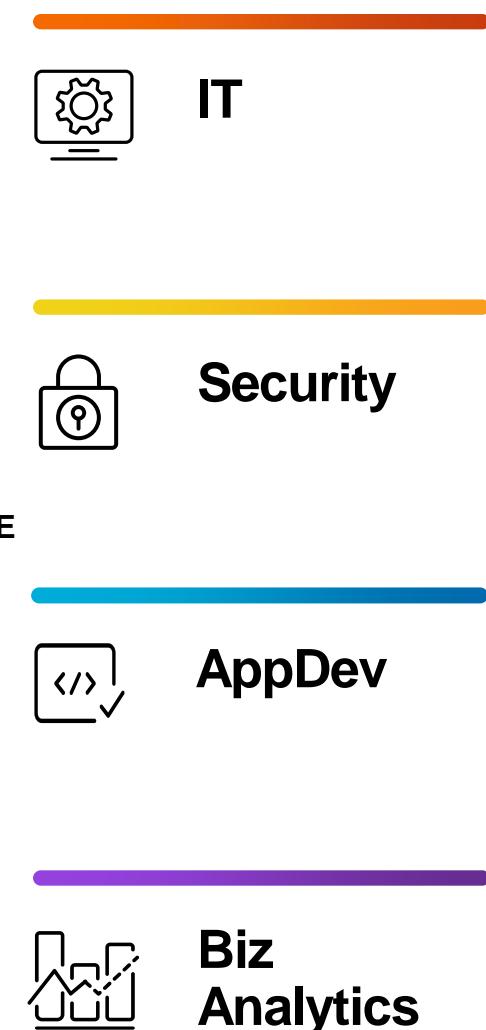


MONITOR

ACT

INVESTIGATE

Any Structure
Any Source
Any Time Scale



Our Investigative Approach

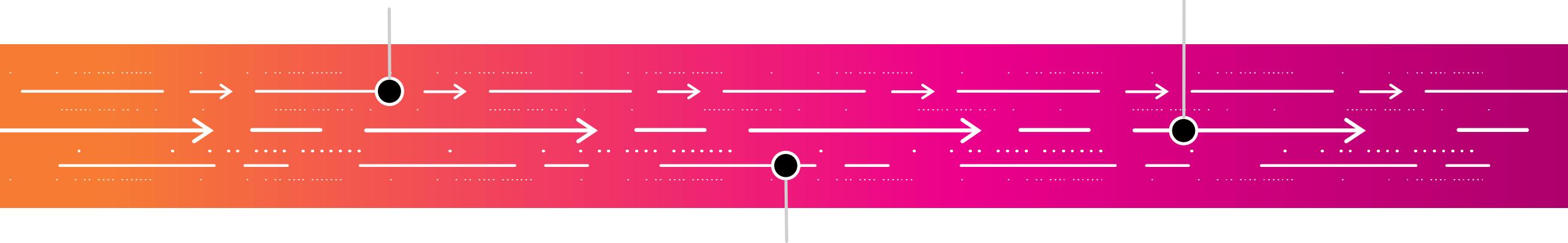
Adaptable | Real-Time | Fast To Value | Massive Scale

Send

unstructured data from all
systems, devices, and people

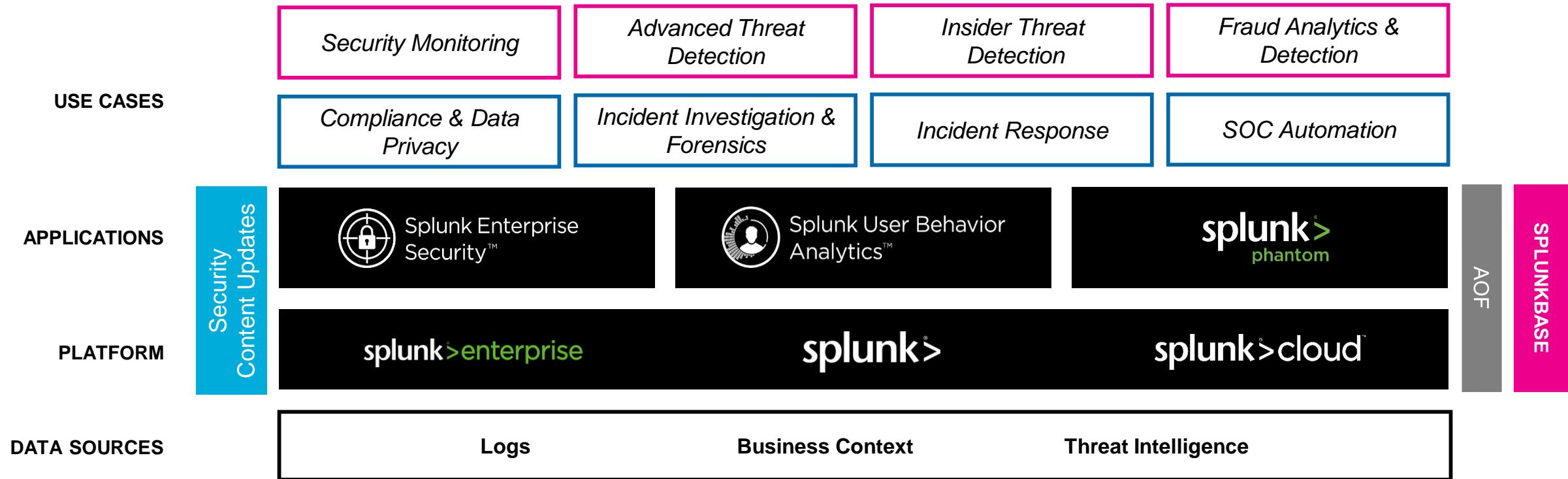
React

quickly to changing circumstances by
asking questions immediately

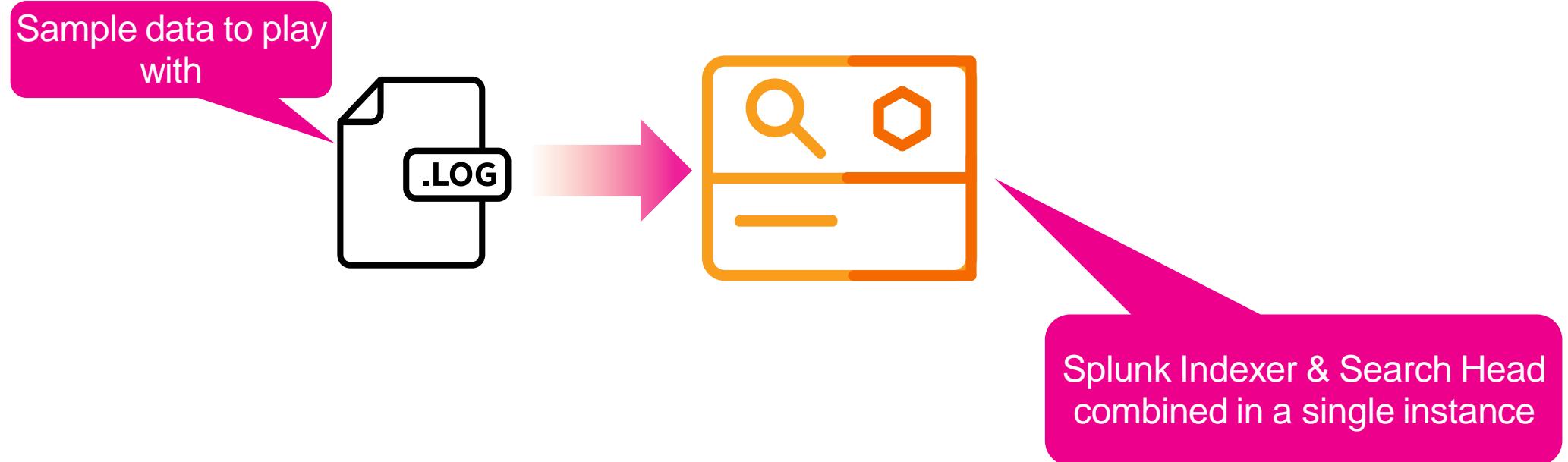


Don't Structure
your data until you are ready

Security Operations Suite

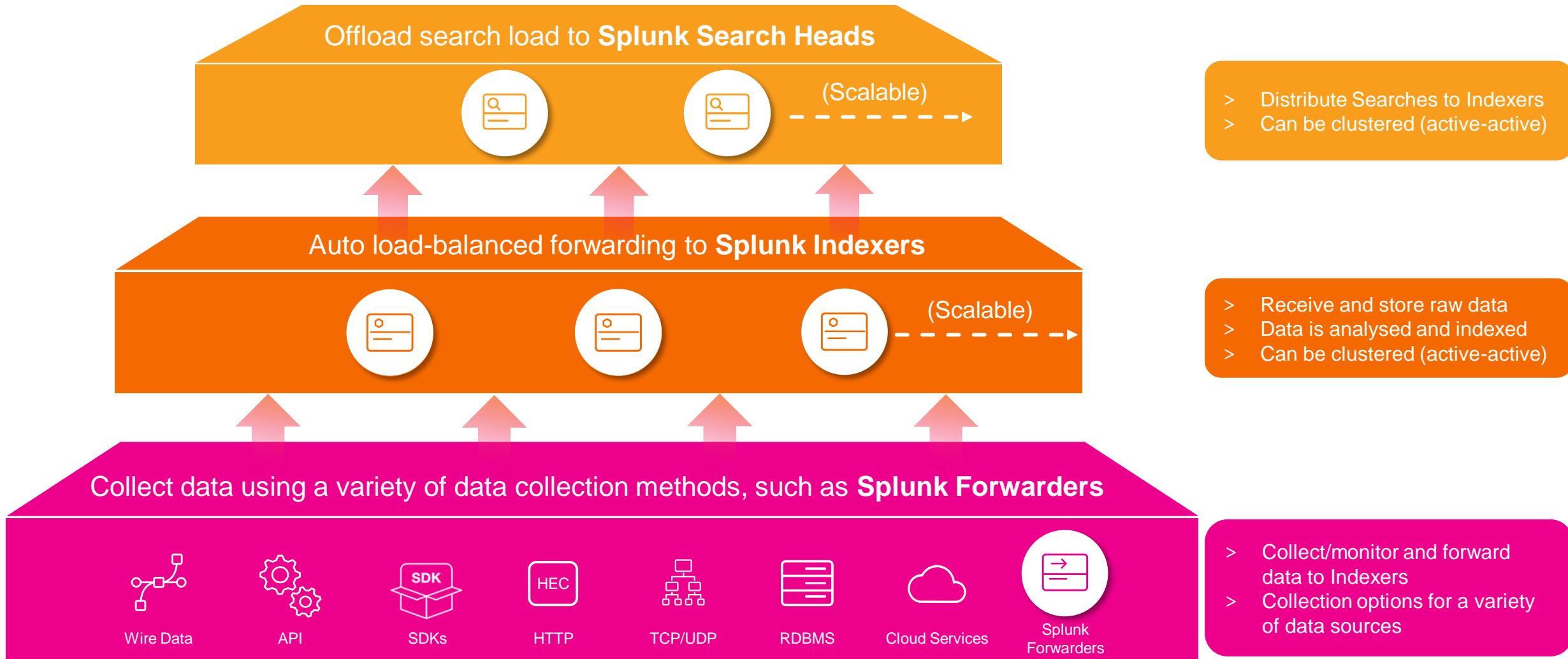


Today's Environment



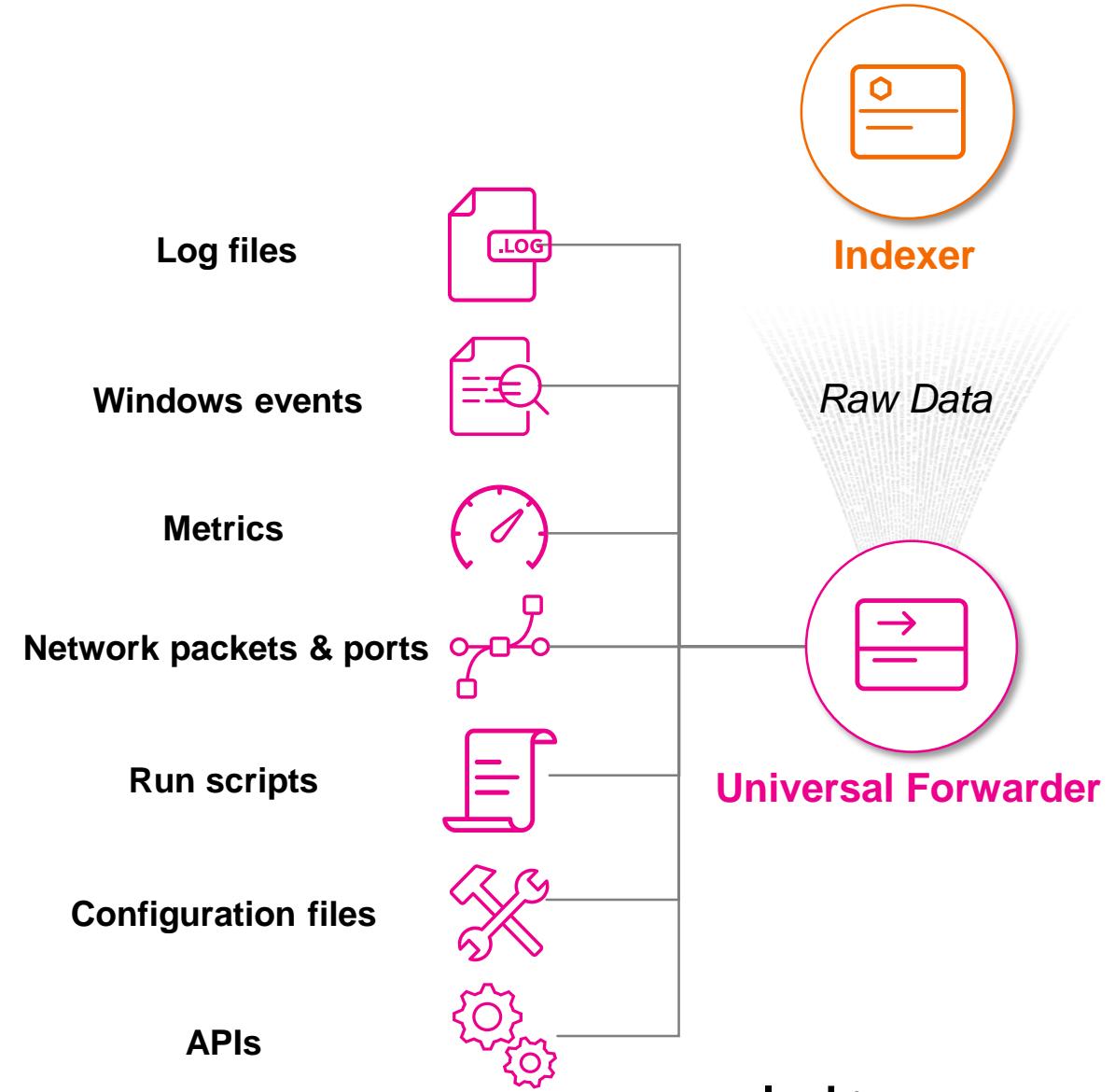
Scales to Petabytes Per Day

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

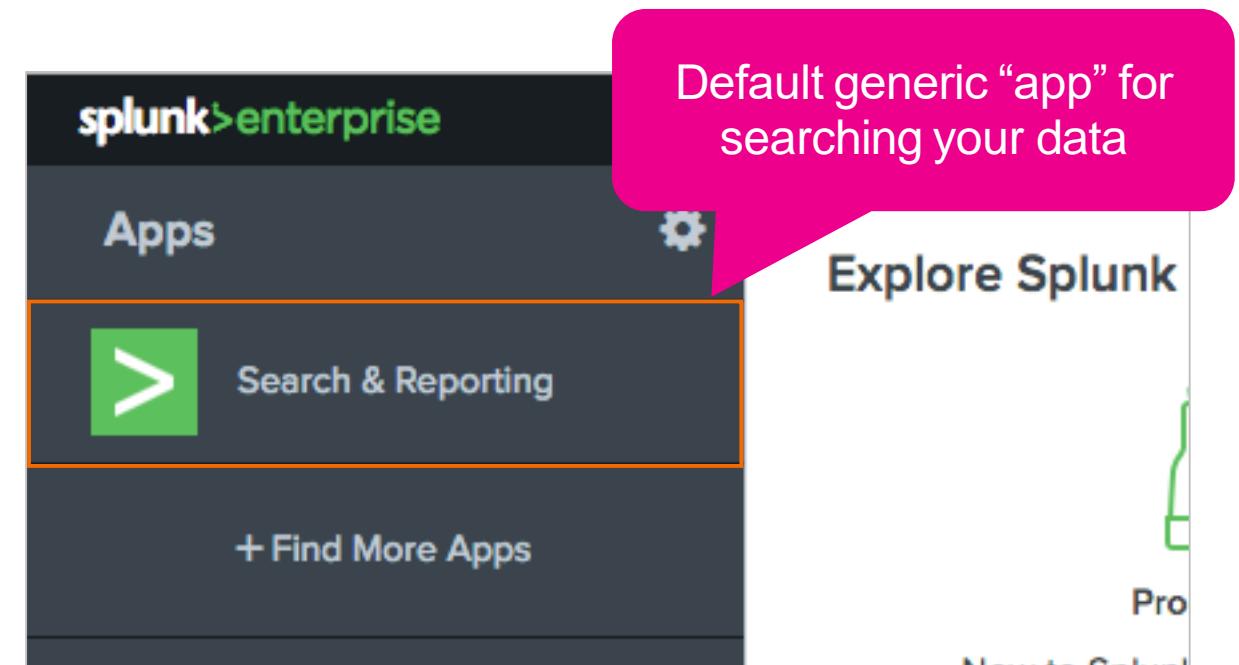
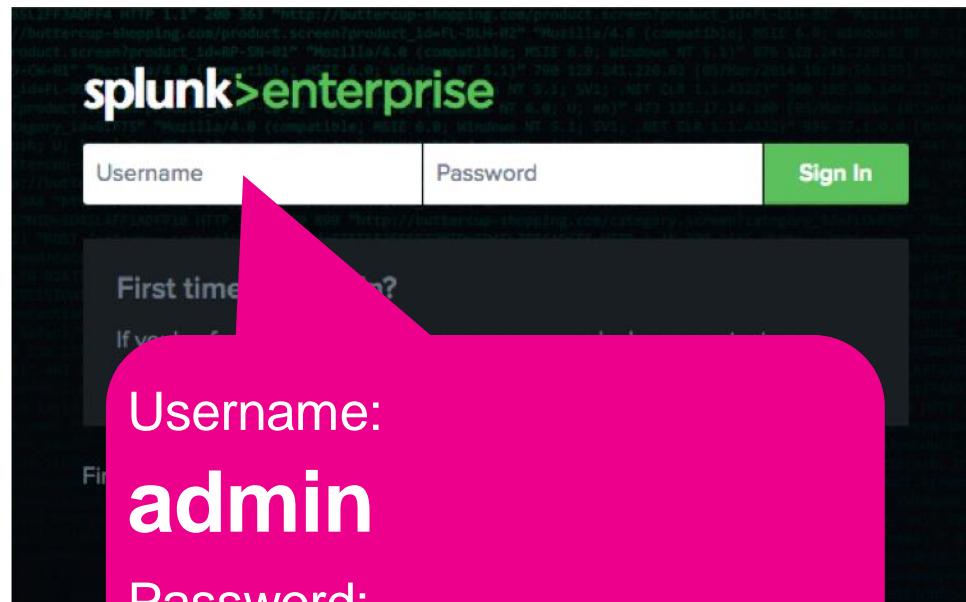
Security Data and Searches

For Security People



Let's Go!

Log in to Splunk



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!



A screenshot of the Splunk web interface. At the top, there's a navigation bar with tabs: Reports, Alerts, Dashboards, Network Diagram, Ready Made Searches (which has a red notification badge with the number 1), and a dropdown arrow. Below the navigation bar, there's a search bar and some search results. A large, semi-transparent pink callout bubble with the text "Click Here!" points to the "Ready Made Searches" tab. The main content area shows a list of search results under the heading "Chapter 1 - Search Basics" (which is highlighted with a blue border and has a red number 2 above it). The results include "Chapter 2 - Field Extraction", "Chapter 3 - EventTypes and", "Chapter 4 - Discovery", and "Chapter 5 - Post Exploit". To the right of this list is another dropdown menu with items like "Chpt1 - Search 1", "Chpt1 - Search 2", etc., each with a magnifying glass icon. A red number 3 is placed next to this second dropdown. The bottom right corner of the interface shows some statistics: "955.8", "INDEXED", and "955.8 / 955.8".

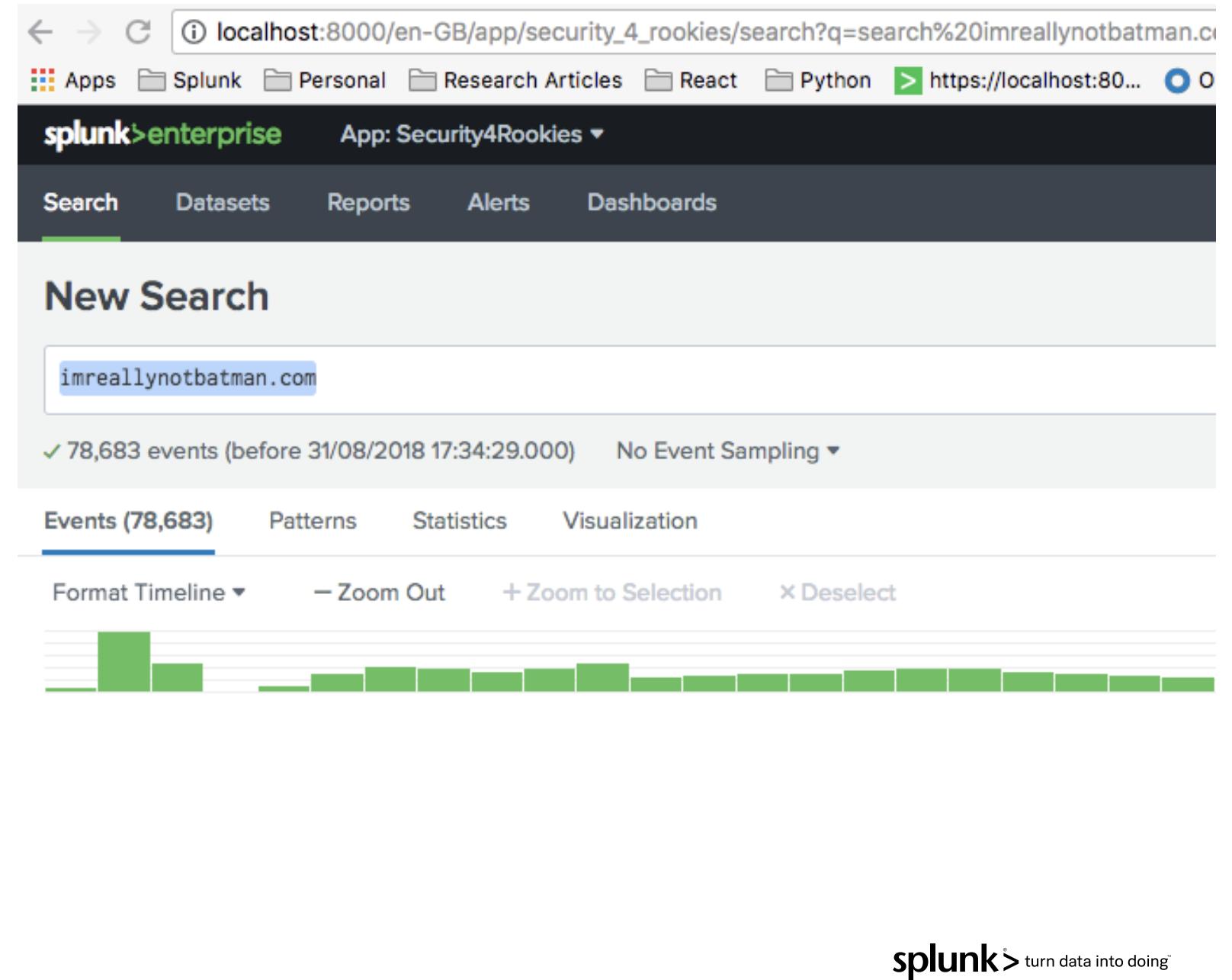
Search Basics

Chpt1 – Search 1

Literal Strings

Manual

imreallynotbatman.com



Search Basics

Chpt1 – Search 2

Key=Value pair searching

Manual

hostname="imreallynotbatman.com"

The screenshot shows the Splunk Enterprise search interface. The URL in the browser bar is `localhost:8000/en-GB/app/security_4_rookies/search?q=search%20hostname%3Dimreal`. The top navigation bar includes links for Apps, Splunk, Personal, Research Articles, React, Python, and a link to `https://localhost:80...`. The main header displays "splunk>enterprise" and "App: Security4Rookies". Below the header, there are tabs for Search, Datasets, Reports, Alerts, and Dashboards, with "Search" being the active tab. A large search bar contains the query `hostname=imreallynotbatman.com`. Below the search bar, it says "13,915 events before 31/08/2018 17:38:03.000" and "No Event Sampling". There are four tabs below the search bar: Events (13,915), Fields, Statistics, and Visualization, with "Events (13,915)" being the active tab. A green bar chart is visible at the bottom. A pink callout bubble on the right side lists "Other Options":

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

Other Options

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

Search Basics

Chpt1 – Search 3

Using OR

Manual

hostname="imreallynotbatman.com"

OR

hostname="www.microsoft.com"

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

localhost:8000/en-GB/app/security_4_rookies/search?earliest=0&latest=&q=search%20hostna... Apps Splunk Personal Research Articles React Python https://localhost:80... Ok

splunk>enterprise App: Security4Rookies ▾

Search Datasets Reports Alerts Dashboards Ready Made Searches ▾

New Search

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

✓ 13,919 events (before 31/08/2018 18:06:33.000) Event Sampling ▾

Events (13,919) Patterns Statistics Visualiz...

Format Timeline ▾ – Zoom Out + Zoom to Selection Deselect

List ▾

Remember Case Sensitivity

hostname="microsoft.com"

NOT the same as

HOSTNAME="microsoft.com"

splunk> turn data into doing

Search Basics

Chpt1 – Search 4

Using Wildcards

Manual

*3791

The screenshot shows the Splunk Enterprise search interface at localhost:8000/en-GB/app/security_4_rookies/search?s=%2FservicesNS%2Fnobody%2Fsearch%2F%252A3791. The search bar contains the query `*3791`. Below the search bar, it says "35 of 304,517 events matched" and "No Event Sampling". There are four tabs: "Events (35)" (which is selected), "Patterns", "Statistics", and "Visualization". Below these tabs are buttons for "Format Timeline", "Zoom Out", "Zoom to Selection", and "Deselect". A timestamp "24 Aug 2016 17:51" is visible in the bottom right corner of the main search area.

Search Basics

Chpt1 – Search 5

Using Wildcards

Manual

3791*exe

The screenshot shows the Splunk Enterprise search interface at localhost:8000/en-GB/app/security_4_rookies/search?q=search%203791*exe&display.page. The search bar contains "3791*exe". Below the search bar, it says "11 events (before 31/08/2018 18:44:01.000) No Event Sampling". The "Events (11)" tab is selected. At the bottom, there are buttons for "Format Timeline", "Zoom Out", "Zoom to Selection", and "Deselect". The results are displayed as a horizontal timeline with green bars representing event times. At the bottom right, there are buttons for "List", "Format", and "20 Per Page".

Search Basics

Chpt1 – Search 6

CIDR Matching

Manual

192.168.250.0/24

Also try

dest_ip=192.168.250.0/24

Could also key=value search
dest_ip=192.168.250.0/24

New Search

192.168.250.0/24

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

Events (65)

Patterns

Statistics

Visualization

Format Timeline ▾

– Zoom Out

+ Zoom to Selection

✗ Deselect

Raw ▾

✓ Format

20 Per Page ▾

◀ Hide Fields

☰ All Fields

SELECTED FIELDS

↳ host 1
↳ source 4
↳ sourcetype 1

INTERESTING FIELDS

↳ control 1
count 9
↳ edit_allowed 1
folder_id 1

↳ i

Event

↳ { [-]

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

splunk > turn data into doing

Search Basics

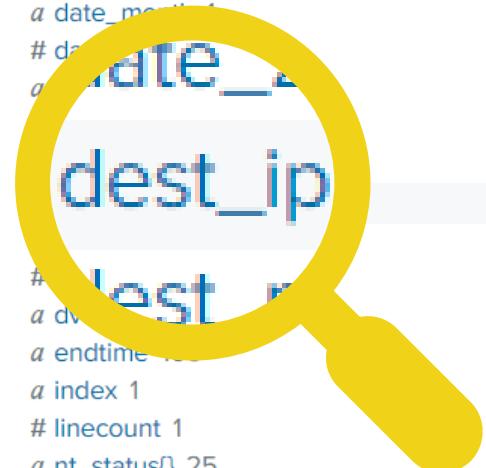
Chpt1 – Search 6

CIDR Matching

Manual

dest_ip=192.168.250.0/24

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



dest_ip

7 Values, 100% of events Selected 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%

L_endtime : 2010-06-24T10:27:45.273003Z , timestamp : 2010-06-24T10:27:27.013472Z"

Splunk's 'Search Processing Language' (SPL)

Search terms

`dest_ip=192.168.250.70`

Commands

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

Pipe character:
Output of left is input to right

e.g. `dest_ip=192.168.250.70`

	Time	Event
>	24/08/2016 18:19:15.000	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>5698FFBD9>/><EventID>3</EventID><Version>5</Version><Level>4</Level><TaskSystemTime>'2016-08-24T18:19:15.575273700Z'</EventRecordID>3705233</Event>crossoft-Windows-Sysmon/Operational</Channel><Computer>we9041srv.waynecorp<='UtcTime'>2016-08-24 18:20:05.127</Data><Data Name='ProcessGuid'>{46C7284='Image'>System</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='Ipv6'>false</Data><Data Name='SourceIp'>192.168.250.20</Data><Data Name='\$Data'><Data Name='SourcePortName'>microsoft-ds</Data><Data Name='Destinat<='DestinationHostname'></Data><Data Name='DestinationPort'>64108</Data><Data Name='host'>we9041srv</Data><Data Name='source'>WinEventLog:Microsoft-Windows-Sysmon/Operational</Data>
>	24/08/2016 18:04:15.000	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>5698FFBD9>/><EventID>3</EventID><Version>5</Version><Level>4</Level><TaskSystemTime>'2016-08-24T18:04:15.604356700Z'</EventRecordID>3701741</Event>crossoft-Windows-Sysmon/Operational</Channel><Computer>we9041srv.waynecorp<='UtcTime'>2016-08-24 18:05:05.126</Data><Data Name='ProcessGuid'>{46C7284='Image'>System</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='Ipv6'>false</Data><Data Name='SourceIp'>192.168.250.20</Data><Data Name='\$Data'><Data Name='SourcePortName'>microsoft-ds</Data><Data Name='Destinat<='DestinationHostname'></Data><Data Name='DestinationPort'>6408</Data><Data Name='host'>we9041srv</Data><Data Name='source'>WinEventLog:Microsoft-Windows-Sysmon/Operational</Data>

Functions

`| 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 audit
EventCode=4689
EventType=0
Type=Information
ComputerName=we8105desk.waynecorpinc.local
TaskCategory=Process Termination
OpCode=Info
RecordNumber=39161
Keywords=Audit Success
Message=A process has exited.

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

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

```

WinEventLog:Security

Multi Line Breaking
Complex Field Extractions
Process ID needs Hex Decoding

```

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

```

fortigate:utm

Single Line Breaking
Key=Value pair Extractions

Extracting Fields Basics

Where you make your data useable

Field Extraction Basics

RULEZ for Field Extraction

- 1) **Technology Addons** are your **fastest** route
(splunkbase.splunk.com) – search Technology AddOns
- 2) Check automatically recognized sourcetypes
(<http://docs.splunk.com/Documentation/Splunk/latest/Data>Listofpretrainedsourcetypes>)
- 3) Key=Value works out the box – use field aliasing if you want to rename
- 4) UI based extraction when 1 – 3 didn't come through for you

Field Extraction Basics

Chpt2 – Search 1

Search your data source

Manual

Index=botsv1 sourcetype=fgt_utm

The screenshot shows two instances of the Splunk web interface. The left instance displays a search results page for the query `index="botsv1" sourcetype="fgt_utm"`. A specific event is selected, and its details are shown in a modal window. The right instance shows the same search results page, but with a context menu open over the selected event. The menu has three options: "Build Event Type", "Extract Fields", and "Show Source". Pink numbers 1, 2, and 3 are overlaid on the interface to indicate the sequence of actions:

- A pink arrow points from the top-left towards the event details in the left panel.
- A pink arrow points from the bottom-left towards the "Event Actions" button in the left panel.
- A pink arrow points from the bottom-right towards the context menu in the right panel.

Event Details (Left Panel):

```

24/08/2016 19:27:14 192.168.250.1 date=2016-08-24 time=12:27:14 devname=gotham-fortigate
vel=information vd="root" appid=1 user="" srcip=192.168.250.41 srcport=51108
srcd=4237598 applist="Honeypot-Access" appcat="Network.Service" app="NTP" action=pass ms=

```

Event Actions (Left Panel):

- Type: Selected

Context Menu (Right Panel):

- Build Event Type
- Extract Fields
- Show Source

Field Extraction Basics

Chpt2 – Search 1

Extract the field

The screenshot shows the Splunk Field Extractor interface at the 'Select Method' step. The URL is `localhost:8000/en-GB/app/security_4_rookies/field_extractor?sid=1535970647.17&offset=0`. The top navigation bar includes links for Apps, Splunk, Personal, Research Articles, React, Python, Okta, Splunk Pwning Portal, Confluence, Service Now, Jira, MITRE ATT&CK, Creating a Splunk J..., and A re-introduction to... . The user is logged in as Administrator.

The main area shows the 'Extract Fields' process with three steps: Select Method (green dot), Select Fields (white dot), and Save (white dot). A green 'Next >' button is at the end of the progress bar. The 'Select Method' section has two options:

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

The source type is set to `fgt_utm`. Below it is a sample log entry:
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=4237598 applist="Honeypot-Access" appcat="Network.Service" app="NTP" action=pass msg="Network.Service: NTP," apprisk=elevated

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

1. Highlight field

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event 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=1056 srcip=192.168.250.1 dstip=91.189.91.157 dstport=123 proto=17 service="NTP" policyid=1 msg=

Extract Require

Field Name 2

Sample 192.168.250.1

Value

Add Extraction 3

1. Highlight field

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

srcip=192.168.250.1

Extract Require

Field Name 2

Sample 192.168.250.1

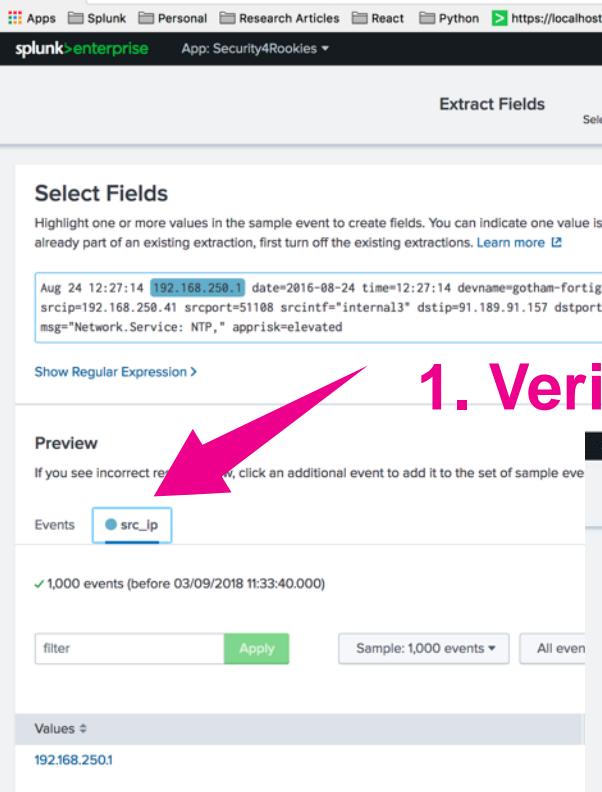
Add Extraction 3

Field Extraction Basics

Chpt2 – Search 1

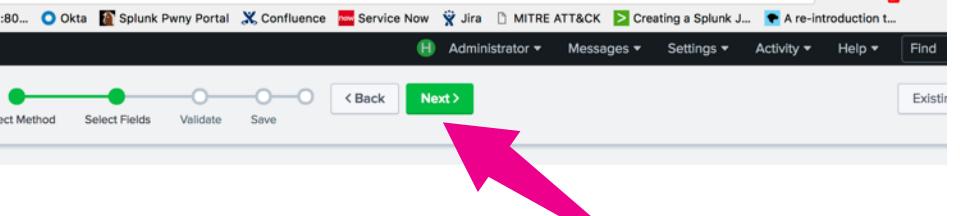
Verify Fields and Set Access Rights

1. Verify Values



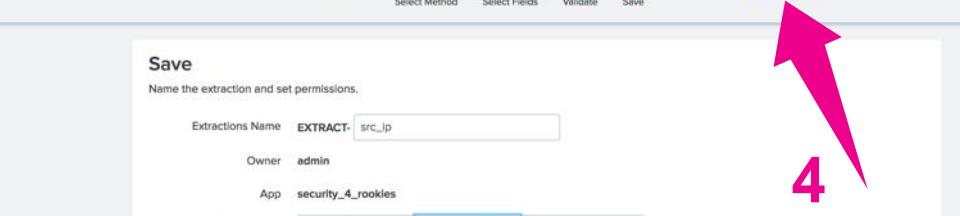
The screenshot shows the 'Extract Fields' wizard in Splunk. The current step is 'Select Fields'. The interface includes a preview of sample event data, a 'Show Regular Expression' button, and a 'Preview' section. In the 'Preview' section, there is a note about incorrect results and a link to add more events. Below this is a 'Events' section with a 'src_ip' button highlighted by a pink arrow. Further down is a 'Values' section containing the IP address '192.168.250.1'.

2. Next Step



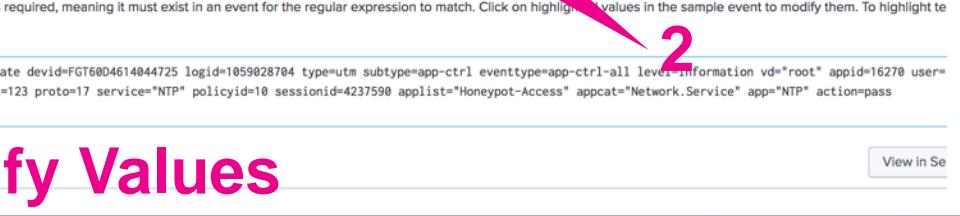
The screenshot shows the 'Validate' step of the wizard. The 'Extract Fields' progress bar has a green dot on 'Select Fields' and a grey dot on 'Validate'. A pink arrow points to the 'Next >' button at the top right.

3. Save Step



The screenshot shows the 'Save' step of the wizard. It displays extraction details like name, owner, app, and source type. Under 'Permissions', the 'App' tab is selected, and a pink arrow points to it. The table shows permissions for various roles like everyone, admin, can_delete, power, and splunk-system-role.

4. Finish Step



The screenshot shows the 'Finish' step of the wizard. The 'Extract Fields' progress bar has green dots on all four steps: 'Select Method', 'Select Fields', 'Validate', and 'Save'. A pink arrow points to the 'Finish >' button at the top right.

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	success	
VPN Logon Success Event	vpn_auth_success		authentication
Windows Logon Failure Event	win_auth_failure		
Linux Logon Failure Event	linux_auth_failure	failure	
VPN Logon Failure Event	vpn_auth_failure		

Event Types & Tags Basics

Chpt3 – Search 1

Creating an Eventtype

Manual

index=botsv1

sourcetype=WinEventLog:Security
(EventCode=4624)

localhost:8000/en-GB/app/security_4_rookies/search?q=search%20index%3D"botsv1"%20sourcetype%3D"WinEventLog:Security"%20(EventCode%3D4624)

splunk>enterprise App: Security4Rookies

Search Datasets Reports Alerts Dashboards Ready Made Searches

New Search

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

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

Events (3,209) Patterns Statistics Visualization

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

List ▾ Format 20 Per Page ▾

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

< Hide Fields All Fields i >

SELECTED FIELDS a host 3

splunk> turn data into doing

Event Types & Tags Basics

Chpt3 – Search 1

Creating an Eventtype

Manual

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

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

2. "Save As"

3. "Event Type"

4. Enter Event Type name "win_auth_success"

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

6. "Save"

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.

Cancel Save

Event Types & Tags Basics

Chpt3 – Search 2

Searching by tags

Manual

tag=authentication tag=success

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

- Search Bar:** tag=authentication tag=success
- Results Summary:** 3,209 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000) No Event Sampling
- Event View:** Shows a single event with fields like Time, LogName, SourceName, EventCode, EventType, and Show all 49 lines.
- Context Menu (opened over the event):**
 - 1. Click “eventtype”
 - 2. Note that our new Event Type is shown
- Selected Fields:** host 3, source 1, sourcetype 1
- Interesting Fields:** Account_Domain 5, Account_Name 12, Authentication_Package, ComputerName 3, EventCode 1, eventtype 1, EventType 1, Impersonation_Level 3, index 1, Key_Length 2, Keywords 1, linecount 3, LogName 1, Logon_GUID 29

Bonus Material

Chpt3 – Search 3

REGEX for the brave

Manual

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

Screenshot of the Splunk Enterprise search interface showing a search results page for the "Security4Rookies" app.

The search bar contains the query: `tag=authentication | rex field=form_data "username=(?P<user>.*?)&.*passwd=(?P<password>.*?)&"`

The search results summary indicates `413 events (10/08/2016 04:28:51.000 to 24.10.2016 19:27:44.000) No Event Sampling`.

The results table has columns: `i` (Info), `Time`, and `Event`. One event is shown:

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

A pink callout bubble highlights the regex pattern `rex field=<field_name> "(?P<>)"` and the full regex expression `rex field=<field_name> "beforepattern(?P<extract_name>field_match)afterpattern"`.

The bottom right corner features the Splunk logo with the tagline "turn data into doing".

Plugging it all together

Where the rubber meets the road

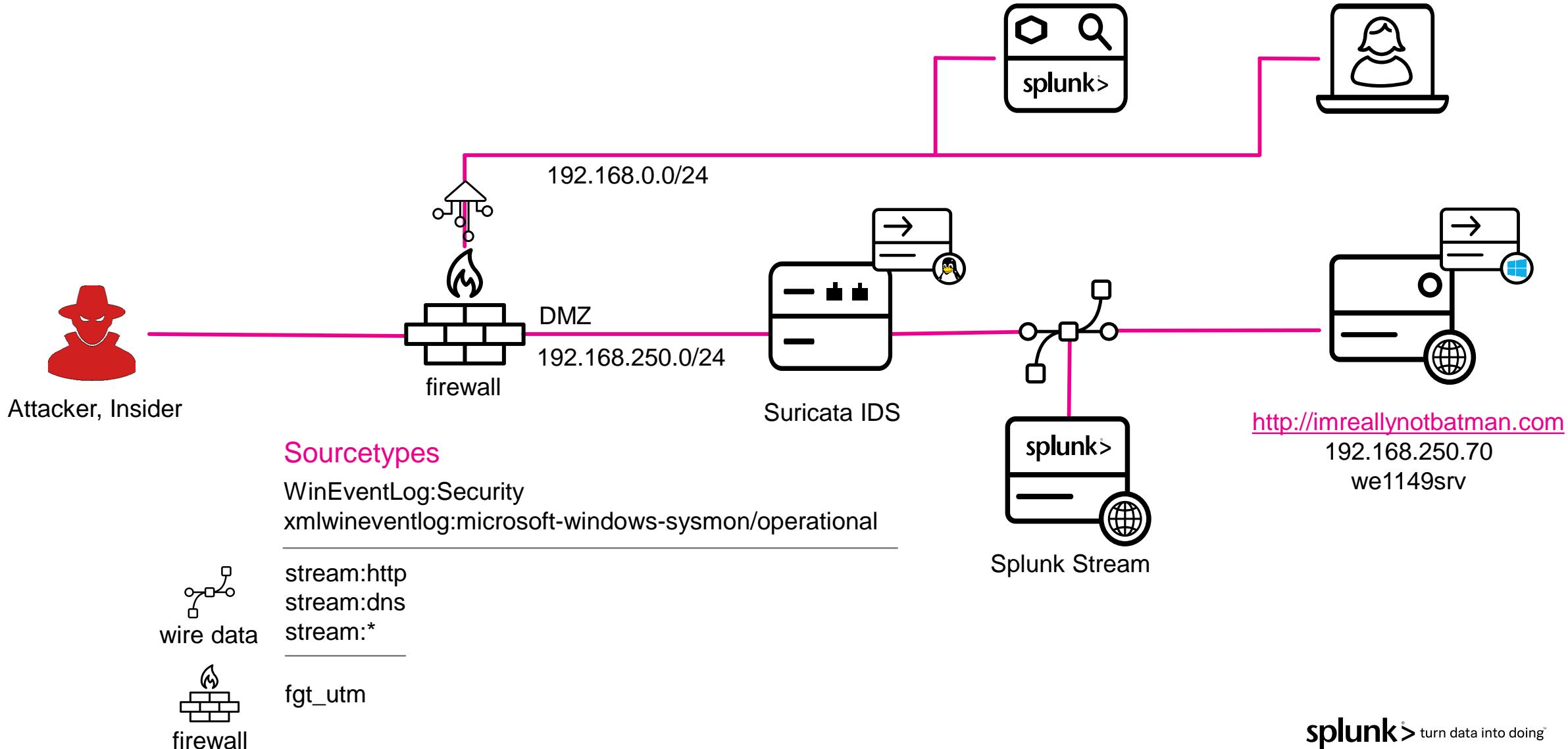
imreallynotbatman.com

Security Data and Searches

For Security People



WayneCorp Network



Discovering the attack

Chpt4 – Search 1

Filter traffic to the web server

Manual

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

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

Stats

Introduction

Examples of stats



| `stats count`

Returns the total number of events on 1 line

| `stats count by src_ip`

Returns the total number of events per src_ip

| `stats min(bytes) avg(bytes) max(bytes) by src_ip`

Returns minimum, average & maximum bytes per src_ip

| `stats dc(src_ip) by dest_ip`

Returns the number of (or distinct) src_ips connecting to dest_ip

| `stats avg(bytes) by _time, src_ip`

Returns average bytes per time slice and src_ip

Discovering the attack

Chpt4 – Search 2

Use stats to aggregate

Manual

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

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

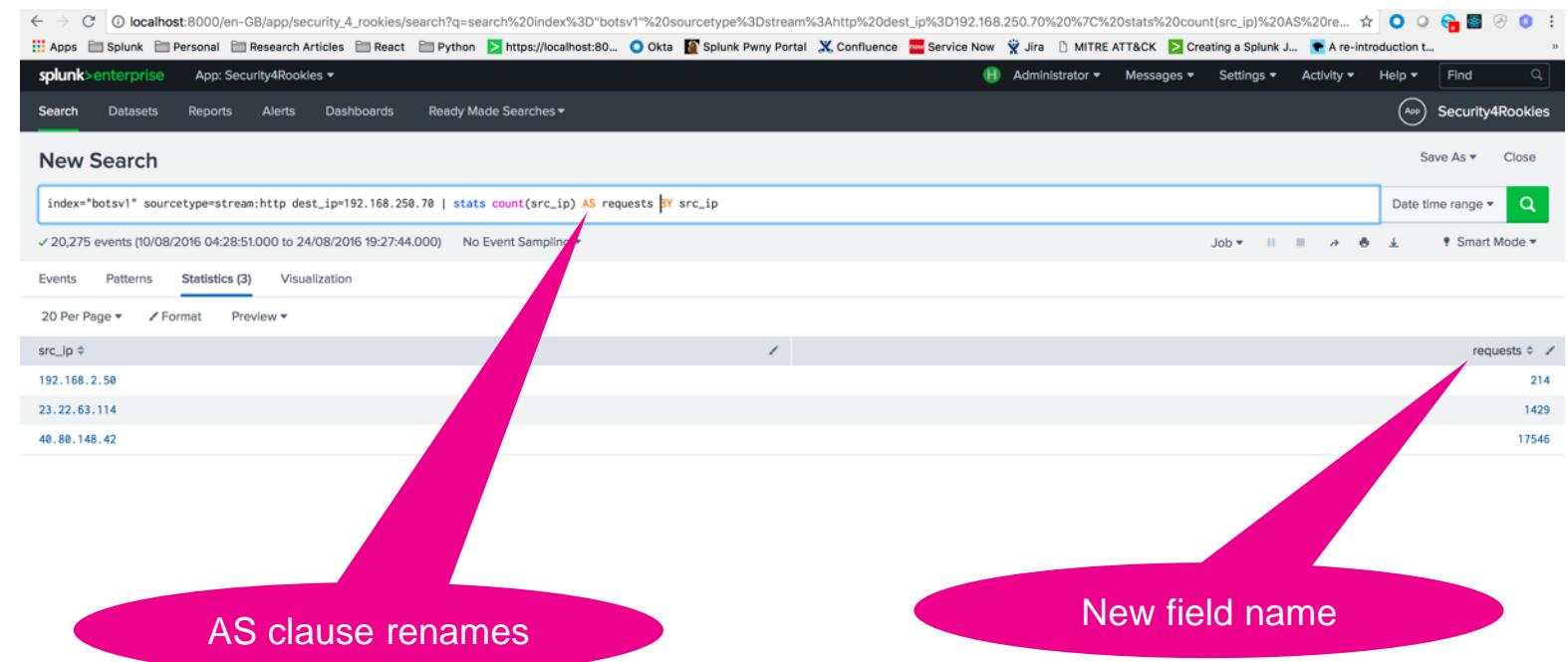
Discovering the attack

Chpt4 – Search 3

Rename fields on the fly

Manual

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



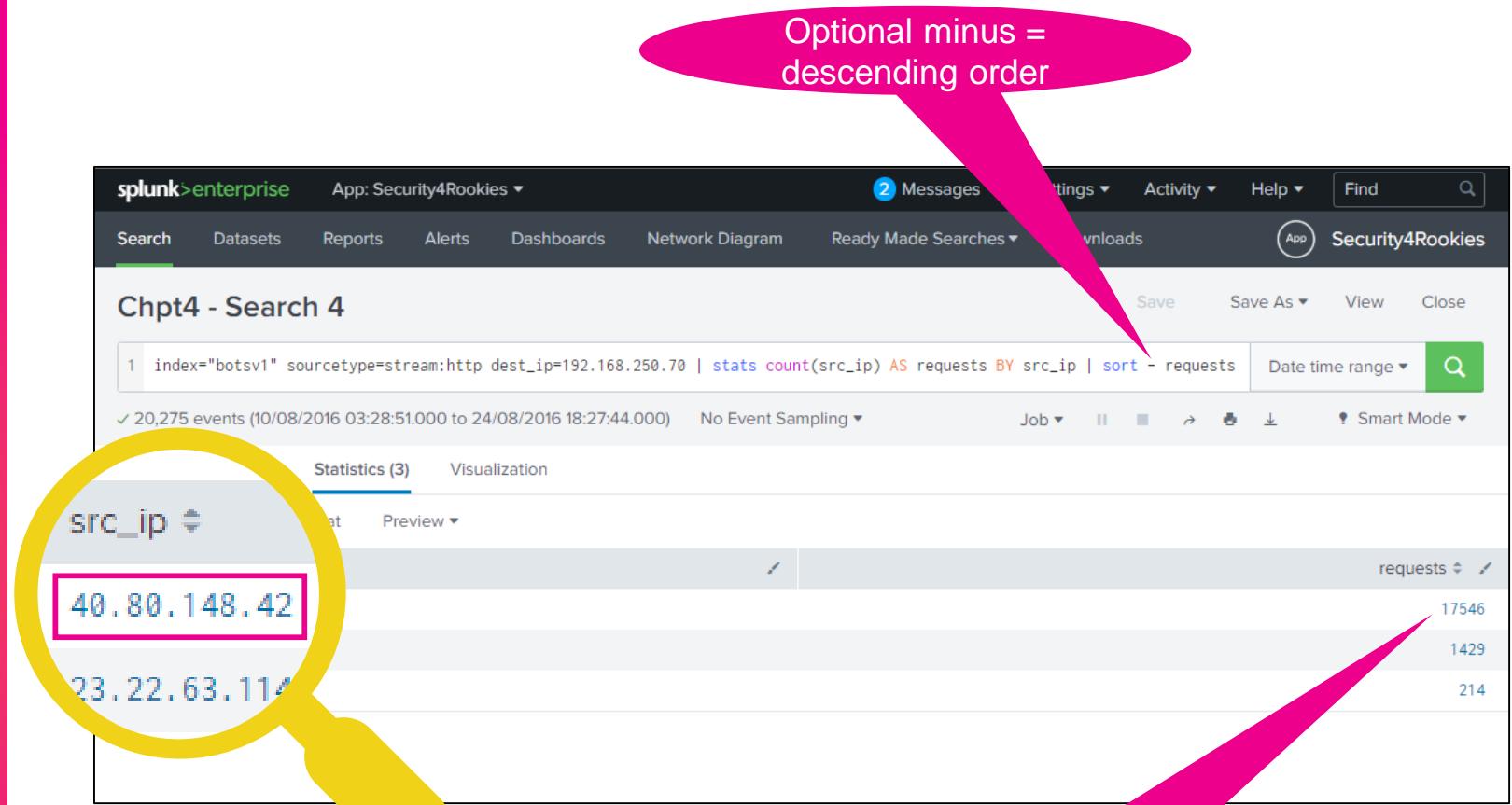
Discovering the attack

Chpt4 – Search 4

Using the sort command

Manual

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



Discovering the attack

Chpt4 – Search 5

Investigating the source headers

Manual

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

Chpt4 - Search 5

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

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

Events (20,275) Patterns Statistics Visualization Format Timeline - Zoom Out + Zoom to Selection Deselect

src_headers

>100 Values, 94.663% of events Selected Yes No

Reports Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
GET /joomla/administrator/index.php HTTP/1.1	412	2.147%
Accept-Encoding: identity Host: imreallynotbatman.com Connection: close User-Agent: Python-urllib/2.7		
GET / HTTP/1.1 Host: 192.168.250.70 Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1 Accept-Language: en Connection: Keep-Alive User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0) Pragma: no-cache Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, */*	88	0.458%
POST /joomla/index.php/component/search/ HTTP/1.1	88	0.458%
Content-Length: 121 Content-Type: application/x-www-form-urlencoded Referer: http://imreallynotbatman.com:80/ Cookie: ae72c62a4936b238523950a4f26f67d0=v7ikbsbiet3vph3 Host: imreallynotbatman.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Acunetix-Product: WVS/10.0 (Acunetix Web Vulnerability Scanner - Free Edition) Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm Accept: */*		

Selected Fields: host 1, source 1, sourcetype 1

Interesting Fields: accept 100+, # ack_packets_in 19, # ack_packets_out 13, # bytes 100+, # bytes_in 100+, # bytes_out 100+, c_ip: 192, cached: 0, canceled: 0, capture_h, client_rt, client_rt, client_rt, connection, cs_pragma, cs_version, data_center, data_packet

Time: 24/08/2016 16:37:13.405

Event:

Scroll down

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
```

The screenshot shows a Splunk search interface titled "Chpt4 - Search 6". 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, http_method | sort - requests`. The results table has three columns: src_ip, http_method, and requests. The data shows 20,275 events from August 10, 2016, to August 24, 2016. The top request is from 40.80.148.42 using POST method with 12844 requests.

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

Discovering the attack

Chpt4 – Search 7

Investigating the data being received

Manual

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

Chpt4 - Search 7

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

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

Events Patterns Statistics (8,612) Visualization

20 Per Page ▾ Format Preview ▾

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

form_data ▾

	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

Discovering the attack

Chpt4 – Search 8

Investigating login activity

Manual

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

1 →

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

- Search Bar:** index="botsv1" sourcetype=stream:http http_method="POST" form_data=*username*passwd*
- Results:** 413 events (10/08/2016 04:28:51.000 to 24/08/2016 19:27:44.000) No Event Sampling
- Event List:** Shows a list of events with columns for Time and Event. One event is selected, showing the timestamp 10/08/2016 22:48:05.858 and the event content: "username=admin&password=arthur".
- Selected Fields:** A list of fields selected for this search, including form_data, index, http_method, and user.
- Field List:** A comprehensive list of all available fields, such as date, dest, and network_interface.
- Reports:** A sidebar with sections for Reports, Top values, and Rare values. A pink callout bubble points to the "Top values" section, which lists several login attempts with the admin user being brute forced.
- Logs:** A sidebar showing log entries related to the search results.

A pink callout bubble highlights the "Top values" section in the Reports sidebar, with the text "Admin user being brute forced".

Value	Count	%
username=admin&password=arthur	1	0.242%
username=admin&password=bigdaddy	1	0.242%
username=admin&password=blazer	1	0.242%
username=admin&password=fire	1	0.242%
username=admin&password=flower	1	0.242%
username=admin&password=fire	1	0.242%
username=admin&password=flower	1	0.242%
username=admin&password=fire	1	0.242%
username=admin&password=flower	1	0.242%

splunk > turn data into doing

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_time 1
# 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
# 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

Reports

[Events with this field](#)

Values

Count %

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

```
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 a Splunk search interface with the following elements:

- Top Bar:** Includes "List", "Format", and "20 Per Page" dropdowns, and a search bar containing the text "1".
- Time Filter:** Shows the current time range as "10/08/2016 21:48:05.858".
- Event Preview:** Displays event details including:
 - _time: 10/08/2016 21:48:05.858
 - accept: text/html, application/xhtml+xml, */*
 - en-US
 - demo-01
 - client_rtt_sum: 82195
 - connection_type: Keep-Alive
 - cookie: 7598a3465c906161e060ac551a9e0276=9qfk26
 - cs_cache_control: no-cache
 - cs_content_length: 111
 - cs_content_type: application/x-www-form-urlencoded
 - cs_version: [[+]
- Time Range Buttons:** Options include "Events Before or After", "Before this time", "After this time" (which is highlighted with a pink box and arrow), and "At this time".
- Nearby Events:** A search bar with "+/- ▾" and "5 second(s) ▾" followed by an "Apply" button.

Post Exploit

Chpt5 – Search 1

Looking for a dropper file

Manual

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

Post Exploit

Chpt5 – Search 2

Investigating Endpoint Processes

Manual

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

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 ▾

< Prev 1 2 3 4

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

Imnotbatman.jpg
overwritten!

Post Exploit

Chpt5 – Search 3

Investigating Web Server Activity

Manual

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

splunk>enterprise App: Security4Rookies ▾

Search Datasets Reports Alerts Dashboards Ready Made Searches ▾

New Search

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

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

Events (7)	Patterns	Statistics	Visualization																		
Format Timeline ▾	<ul style="list-style-type: none"> <i>a</i> http_content_type 1 <i>a</i> http_method 1 <i>a</i> index 1 # linecount 1 # missing_packets_in 1 # missing_packets_out 1 <i>a</i> network_interface 1 # packets_in 2 # packets_out 2 <i>a</i> punct 2 # reply_time 6 <i>a</i> request 4 # request_ack_time 7 # request_time 3 # response_ack_time 5 # response_time 3 cache_control 1 	<i>src_ip: 192.168.250.70 src_mac: 00:0C:29:C4:02:7E src_port: 63139</i>	request 4 Values, 100% of events <input checked="" type="checkbox"/> Selected <input type="checkbox"/> Yes <input type="checkbox"/> No																		
		Reports Top values Top values by time Rare values Events with this field	Values <table border="1"> <thead> <tr> <th></th> <th>Count</th> <th>%</th> </tr> </thead> <tbody> <tr> <td>GET /core/list.xml HTTP/1.1</td> <td>2</td> <td>28.571%</td> </tr> <tr> <td>GET /jed/list.xml HTTP/1.1</td> <td>2</td> <td>28.571%</td> </tr> <tr> <td>GET /poisonivy-is-coming-for-you-batman.jpeg</td> <td>2</td> <td>28.571%</td> </tr> <tr> <td>HTTP/1.1</td> <td></td> <td></td> </tr> <tr> <td>core/extensions/com_joomlaupdate.xml</td> <td>1</td> <td>14.286%</td> </tr> </tbody> </table>		Count	%	GET /core/list.xml HTTP/1.1	2	28.571%	GET /jed/list.xml HTTP/1.1	2	28.571%	GET /poisonivy-is-coming-for-you-batman.jpeg	2	28.571%	HTTP/1.1			core/extensions/com_joomlaupdate.xml	1	14.286%
	Count	%																			
GET /core/list.xml HTTP/1.1	2	28.571%																			
GET /jed/list.xml HTTP/1.1	2	28.571%																			
GET /poisonivy-is-coming-for-you-batman.jpeg	2	28.571%																			
HTTP/1.1																					
core/extensions/com_joomlaupdate.xml	1	14.286%																			
			<i>client_rtt: 202 client_rtt_packets: 1 client_rtt_sum: 202 cs_version: 1.0 data_center_time: 0</i>																		

More Badness!

1

splunk> turn data into doing

Post Exploit

Chpt5 – Search 3

Investigating Web Server Activity

Manual

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

	Event
a c_ip 1	c_ip: 192.168.250.70
# 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	
	i
	Event
	c_ip: 192.168.250.70
	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

Fetching jpeg

DDNS Site

Dashboards

My Manager wants them now! - OK

Dashboards

Chpt6 – Search 1

Brute Force Activity
into our web site

Manual

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

The screenshot shows the Splunk interface with a search results page for 'Chpt6 - Search 1'. The search bar contains the query: `tag=authentication | rex field=form_data "username=(?P<user>.*?)&.*passwd=(?P<password>.*?)&" | chart dc(password) AS numPasswords BY host, user | sort - numPasswords`. The results table shows various hosts and their password attempt counts. A context menu is open at the top right, with the 'Save As' option selected. A large callout diagram with numbered arrows (1 through 7) guides the user through the save process:

- Arrow 1 points to the 'Save As' button in the top right corner of the search results page.
- Arrow 2 points to the 'Dashboard Panel' option in the 'Save As' dropdown menu.
- Arrow 3 points to the 'Dashboard' dropdown in the 'Save As Dashboard Panel' dialog, which is set to 'New'.
- Arrow 4 points to the 'Dashboard Title' input field, which is filled with 'Security Operations'.
- Arrow 5 points to the 'Dashboard Permissions' section, where 'Shared in App' is selected.
- Arrow 6 points to the 'Panel Content' section, which is set to 'Statistics Table'.
- Arrow 7 points to the 'Save' button at the bottom right of the dialog.

The bottom right corner of the image features the Splunk logo with the tagline 'turn data into doing'.

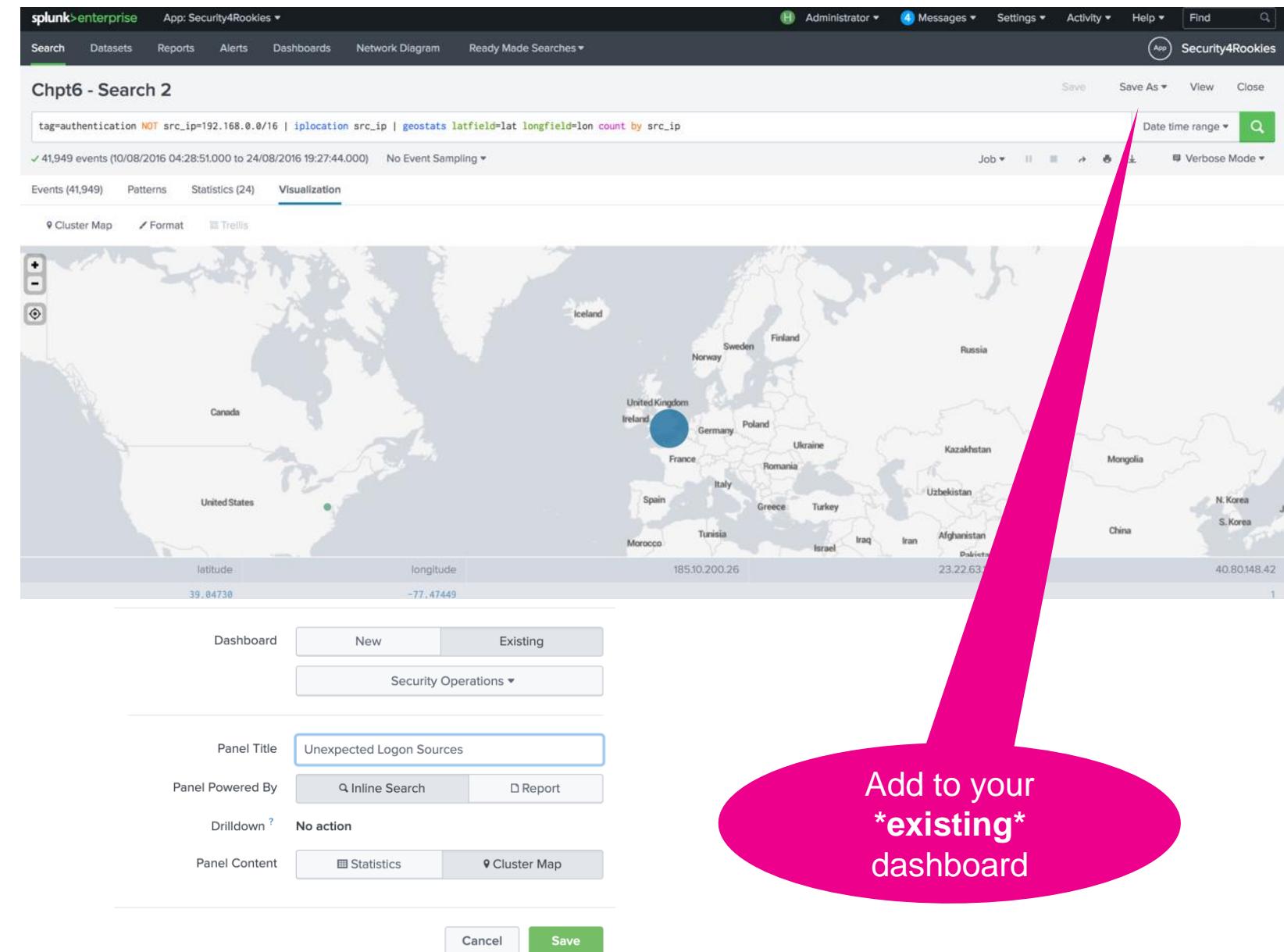
Dashboards

Chpt6 – Search 2

Unexpected Logon Sources

Manual

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



Add to your
existing
dashboard

Dashboards

Chpt6 – Search 3

Analyzing user agent lengths

Manual

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

splunk>enterprise App: Security4Rookies ▾

Administrator 4 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

Search Datasets Reports Alerts Dashboards Network Diagram Ready Made Searches ▾

App Security4Rookies

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

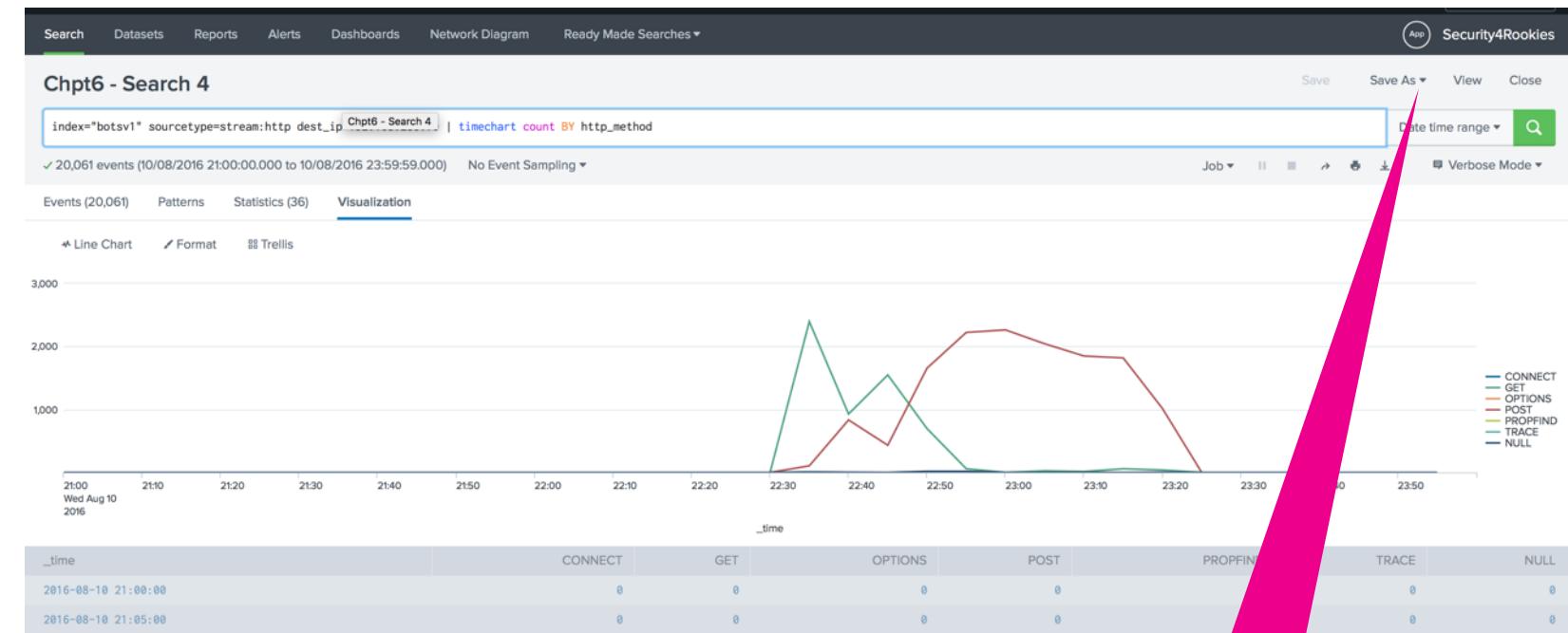
Dashboards

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

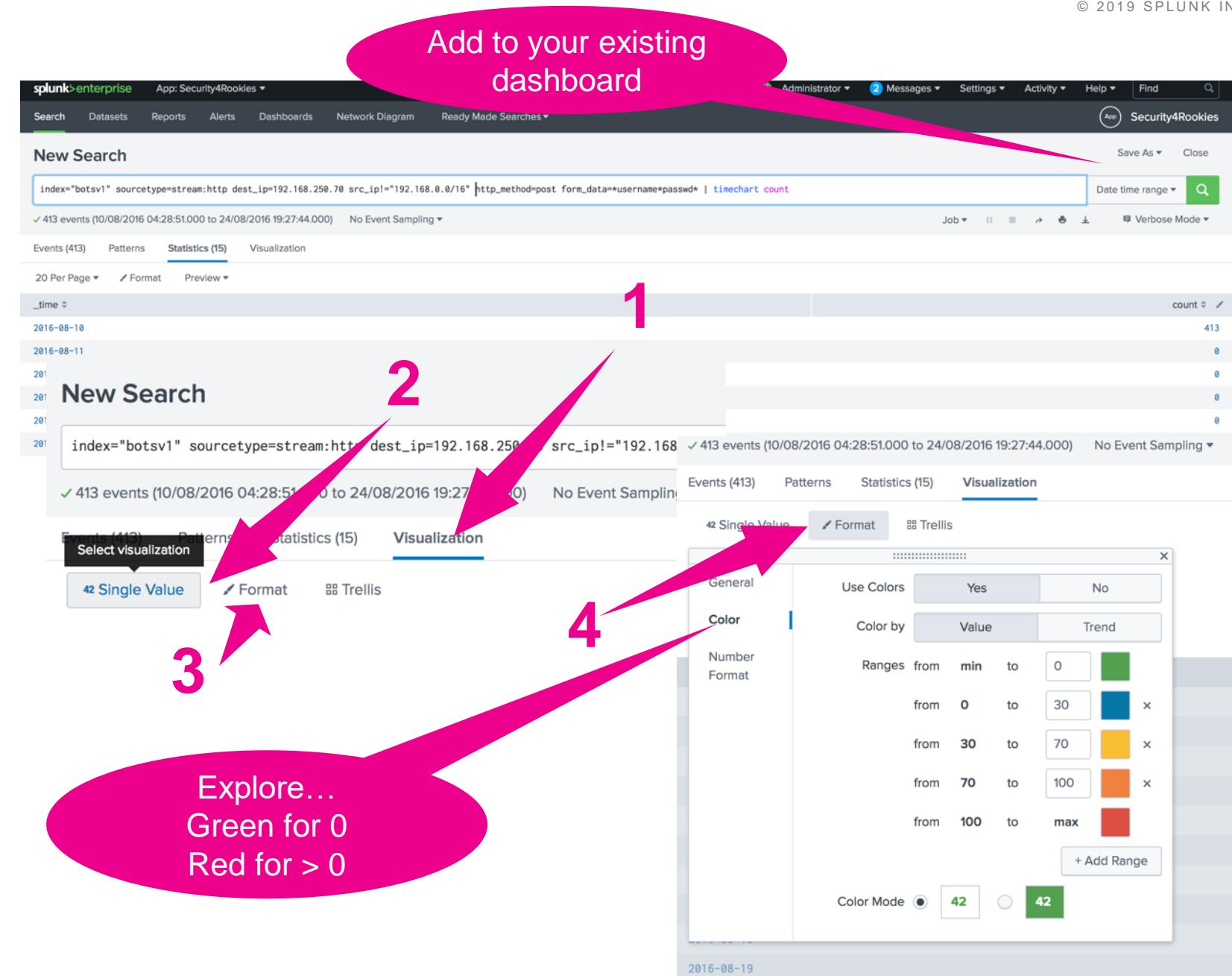
Dashboards

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

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

42 Single Value ✓ Format Trellis

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

42 Single Value ✓ Format Trellis

General Use Colors Yes No

Color by Value Trend

Ranges from min to 0

from 0 to max

+ Add Range

Color Mode 42 42

Explore... Green for 0 Red for > 0

Dashboards

Visualizations

Interactive

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

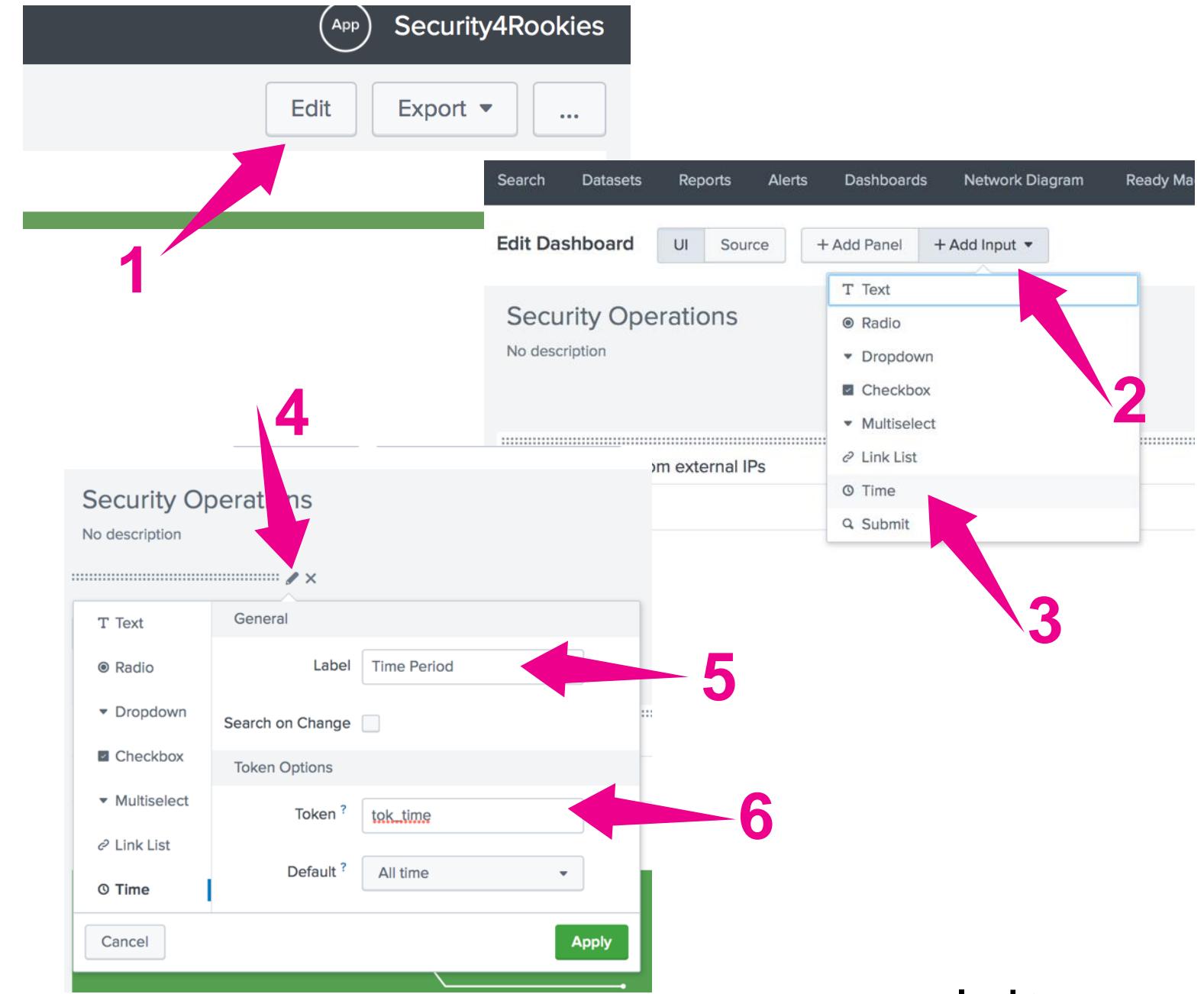
- Header:** splunk>enterprise App: Security4Rookies ▾
- Top Navigation:** Search, Datasets, Reports, Alerts, Dashboards, Network Diagram, Ready M...
- Search Results:** A search for "Dashboards" returns 2 results:
 - Network Diagram
 - Security Operations
- Selected Dashboard:** The "Security Operations" dashboard is currently selected, showing a table titled "Password attempts per user".
- Dashboard Header:** Security Operations
- Dashboard Content:** Password attempts per user table with data:

host	user	numPasswords
splunk-02	admin	344
- Bottom Right:** Edit, Export ▾, ... buttons

Dashboards

Visualizations

Add time selector



Dashboards

Visualizations

Make panels react

The screenshot shows the Splunk dashboard editor interface. At the top, there's a 'Time Period' dropdown set to 'All time'. Below it is a panel titled 'Website logons from external IPs'. A gear icon in the top right corner of this panel is highlighted with a pink arrow labeled '1'. A callout bubble points to it with the text 'Edit search'. The panel itself has a green header bar. In the center, there's an 'Edit Search' dialog box. Inside, the 'Search String' field contains the following SPL query:

```
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
```

Below the search string, the 'Run Search' button is visible. To its right, a dropdown menu for 'Time Range' is open, showing options like 'Use time picker', 'Shared Time Picker (tok_time)', and 'Use time picker' (which is checked). This dropdown is highlighted with a pink arrow labeled '2'. Another pink arrow labeled '3' points to the 'Use time picker' option in the dropdown. A large pink oval on the right side of the screen contains the text 'Repeat for all panels'. A final pink arrow labeled '4' points to the 'Apply' button at the bottom right of the 'Edit Search' dialog.

Dashboards

Visualizations

Changing Visualization Type

The screenshot shows the Splunk Visualization editor interface. At the top, there is a search bar and a toolbar with icons for search, edit, and more. Below the toolbar is a table titled "Password attempts per user" with several columns and rows of data. A pink arrow labeled "1" points to the number "1" in the bottom right corner of the table.

In the center, there is a "Splunk Visualizations" panel containing a grid of visualization icons. One icon, a column chart, is highlighted with a blue border. A pink arrow labeled "2" points to this highlighted icon.

Below the visualization panel is a section titled "Column Chart". On the right side of this section, there is a configuration panel with tabs for "General", "Stack Mode", "Multi-series Mode", "X-Axis", "Y-Axis", "Chart Overlay", and "Legend". The "General" tab is currently selected. A pink arrow labeled "3" points to the "Stack Mode" tab.

Dashboards

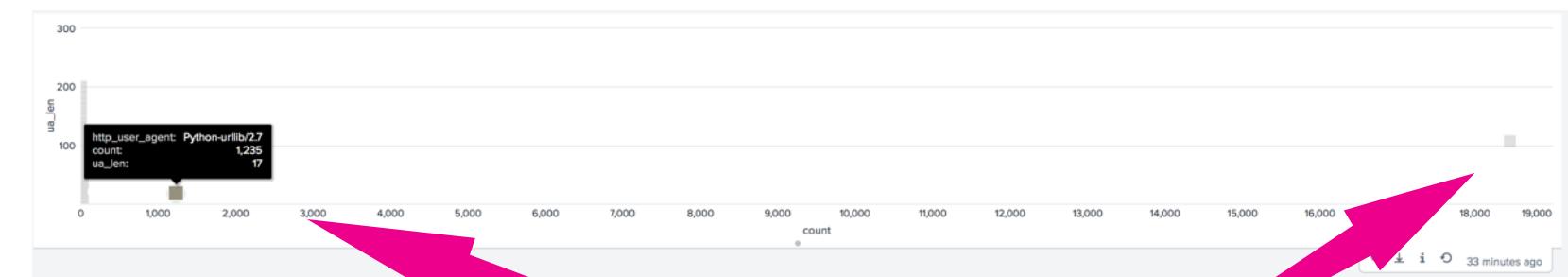
Visualizations

Bonus Challenge

Change http_user_agent panel to a scatter chart

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

YUK! – Wrong type of vis for the data!

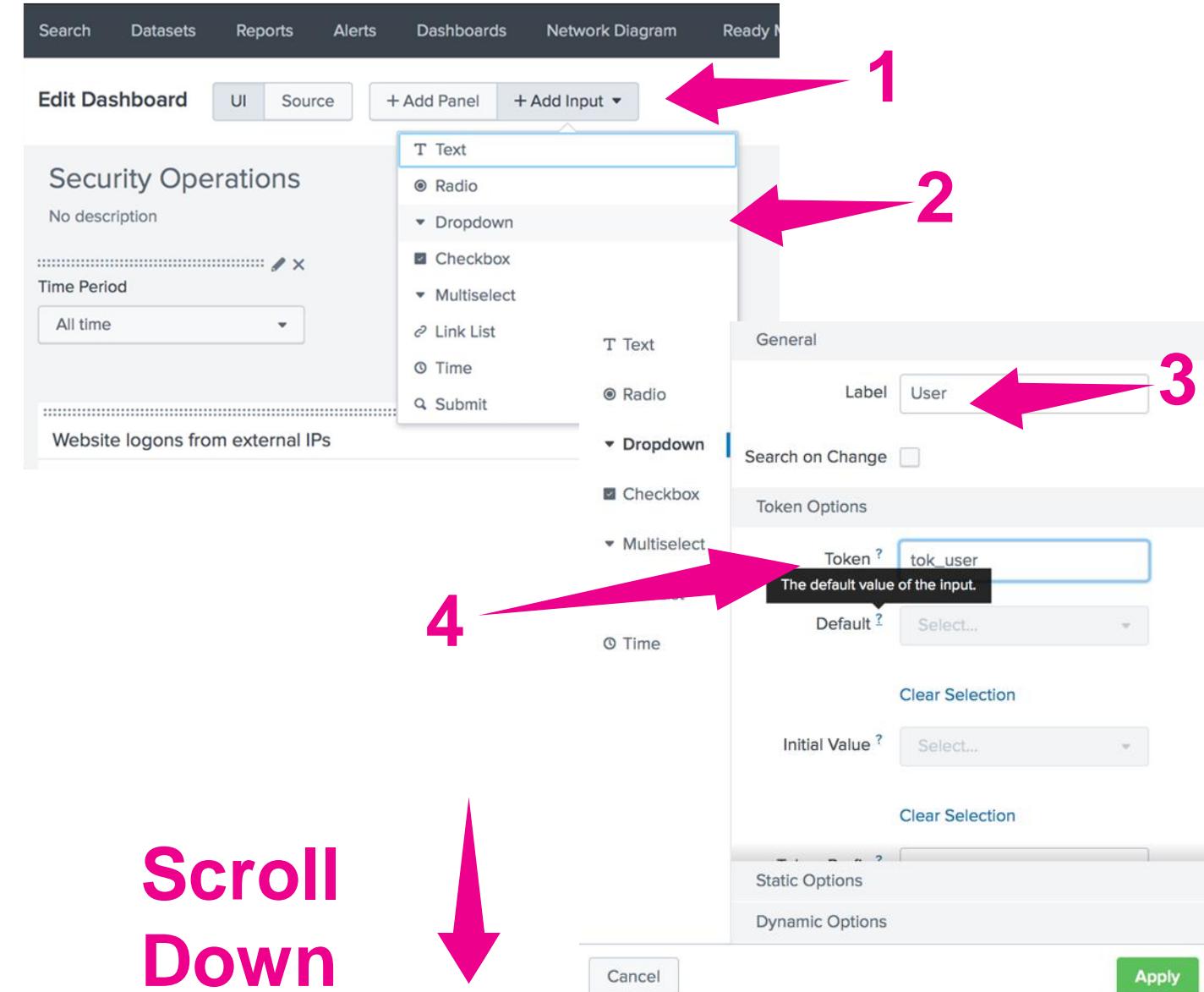


Rare features stand out with good visualizations

Dashboards

Visualizations

Interactive Filtering



Scroll
Down

Dashboards

Visualizations

Continued

Static Options

Name	Value
ALL	*

+ Add New

Dynamic Options

Content Type

Search String

Run Search [Run Search ↗](#)

Last 24 hours

Field For Label [?](#)

Field For Value 7

8 NOT YET!

5 6 Apply

NOT YET!

5

6

7

8

NOT YET!

Apply

Dashboards

Visualizations

Continued

Token Options

Token ? X

Default ? ALL X

Clear Selection

Initial Value ? ALL X

Clear Selection

Token Prefix ?

Scroll Back Up!

9

10

11

T Text
Radio
Dropdown
Checkbox
Multiselect
Link List
Time

General
Token Options
Static Options
+ Add New
Dynamic Options

Content Type X

Search String
Run Search Run

Last 24 hours ▼

Field For Label ?

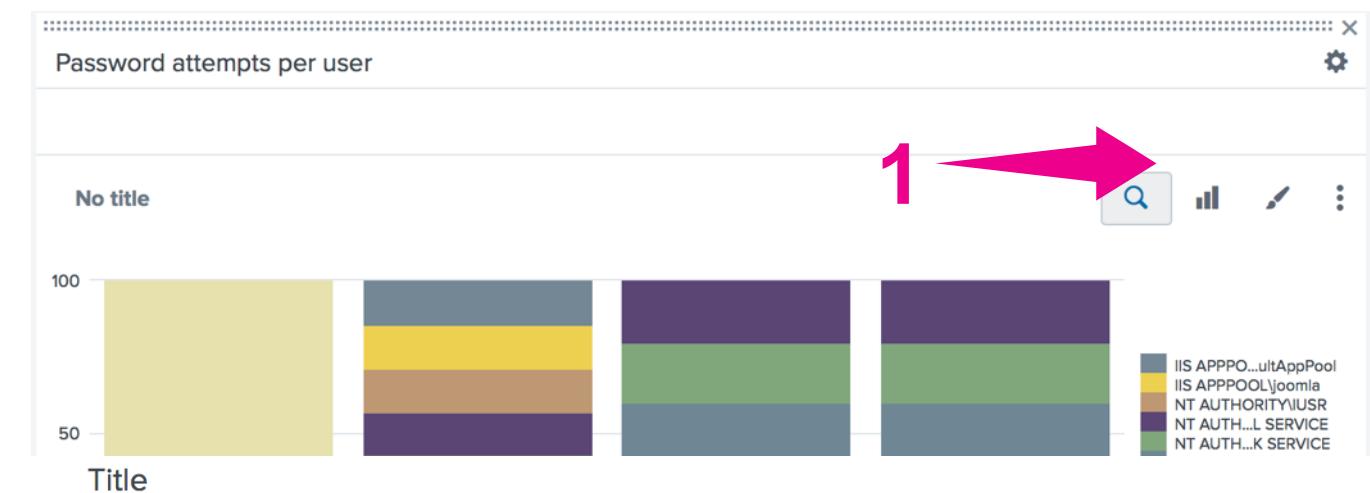
Field For Value ?

C Cancel Apply

Dashboards

Visualizations

Substitute tokens into a dashboard search



Search String

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

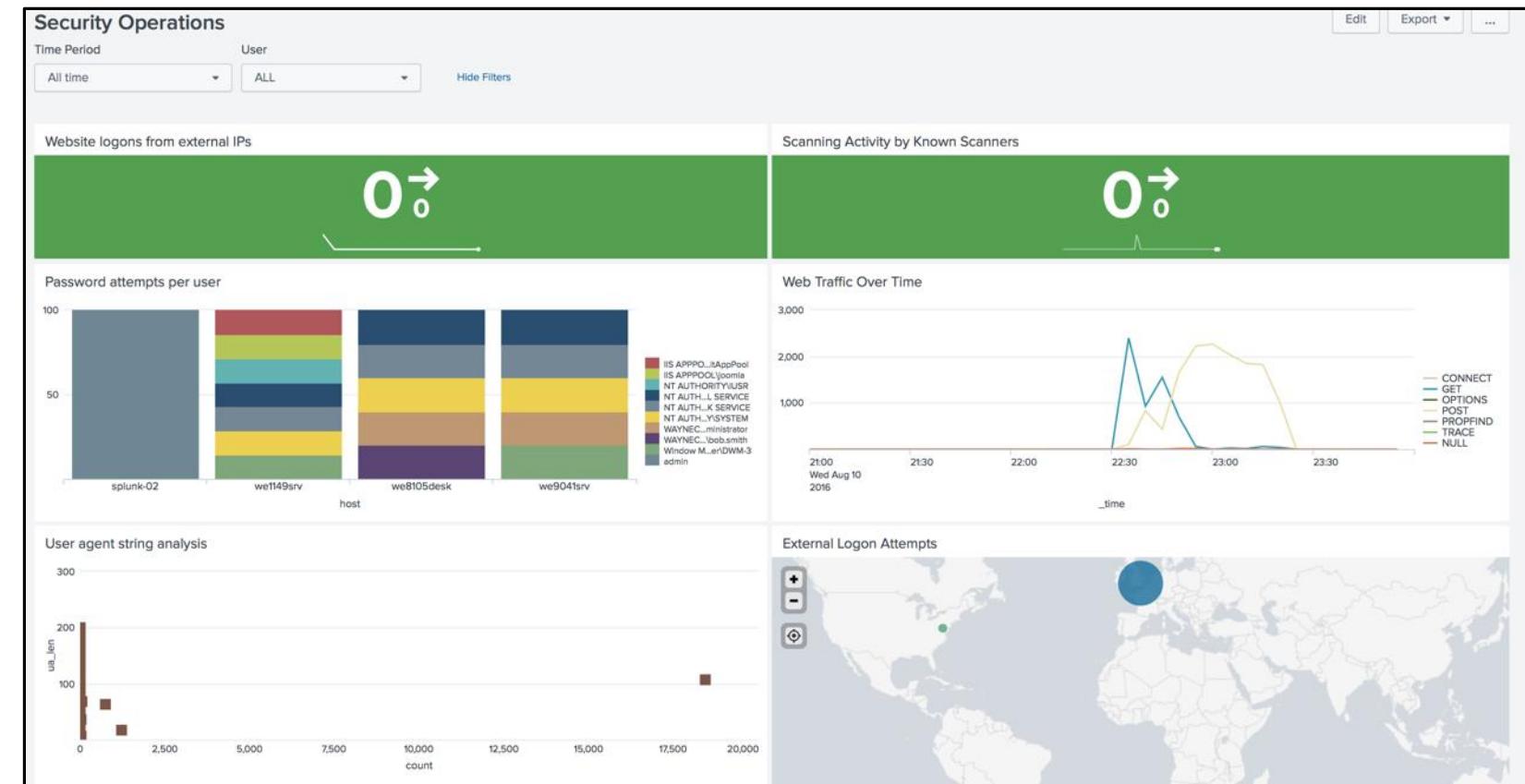
Run Search ↗

ADD
“**search user=\$tok_user\$ |**”

Dashboards

Dashboard Hero

And.... Breathe!



Splunk Resources

Resources

Helpful ‘Stuff’

- 1) Splunk command ‘cheat sheet’**
<https://www.splunk.com/pdfs/solution-guides/splunk-quick-reference-guide.pdf>
- 2) App for Security Monitoring**
<https://splunkbase.splunk.com/app/4131/>
- 3) App for Security Essentials**
<https://splunkbase.splunk.com/app/3435/>
- 4) Splunk Accredited Education**
<https://www.splunk.com/view/SP-CAAAH9U>
- 5) Free Splunk Education!**
https://www.splunk.com/en_us/training/free-courses/splunk-fundamentals-1.html
- 6) Splunk Documentation**
<http://docs.splunk.com/>

Need more inspiration? Security Dataset Project



SPLUNK SECURITY DATASET PROJECT

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

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

Overview ▾ Web-Shells ▾ Supplemental Material ▾ Search Investigating MACCDC

Export ▾ ...

Interested?

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

Email Address: *

[View Details](#)

First Name: *

Last Name: *

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

Todays Content

Download and play

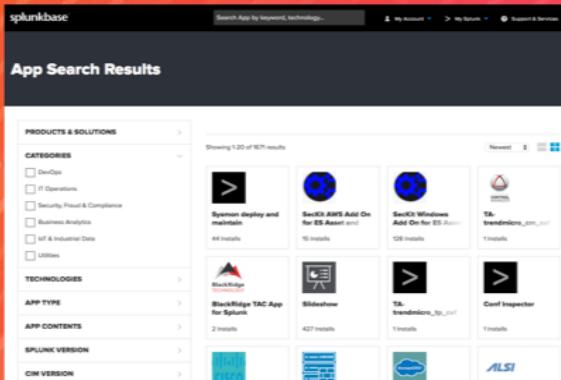
The screenshot shows a Splunk web interface with a dark header bar. In the top right, there are links for "Research Articles", "React", "Python", "https://localhost:8...", "Okta", "Splunk Pwny Portal", and "Cor". The header also displays the user "Administrator" and a "Messages" notification count of 3. Below the header is a navigation bar with tabs: "Alerts", "Dashboards", "Network Diagram", "Ready Made Searches", and "Downloads". The "Downloads" tab is highlighted with a green underline. The main content area contains several items:

- A link to a "Powerpoint presentation presented today".
- A link to a "Security 4 Rookies app, to install on your phone".
- A link to download the app, with the text "In please Download from here." followed by a download button.

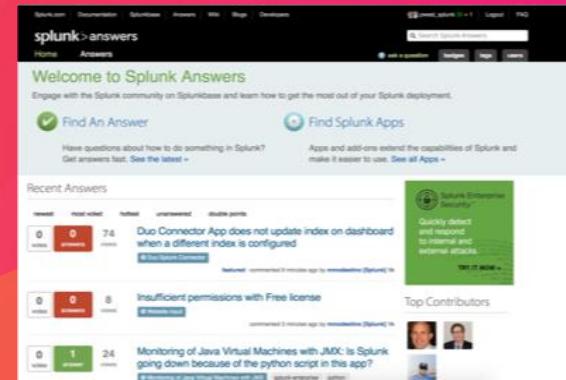
A large, semi-transparent pink circle with a white outline is overlaid on the page, containing the text "Click Here!". A pink arrow points from the top right towards this circle, originating from the "Downloads" tab in the header.

Thriving Community

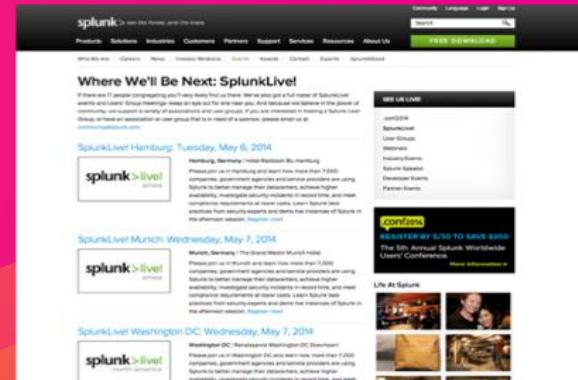
Splunkbase



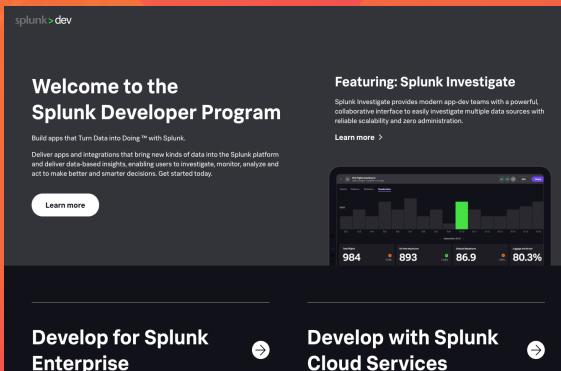
Splunk Answers



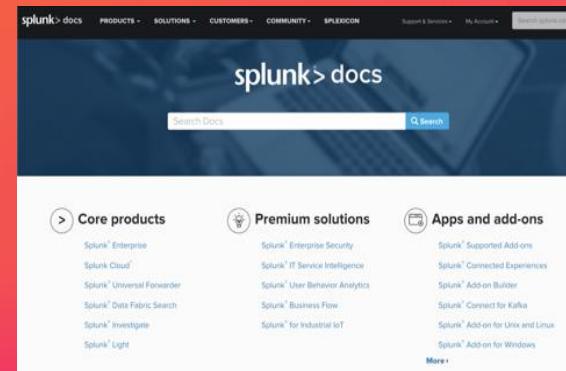
Splunk Events



Developer Resources



Documentation



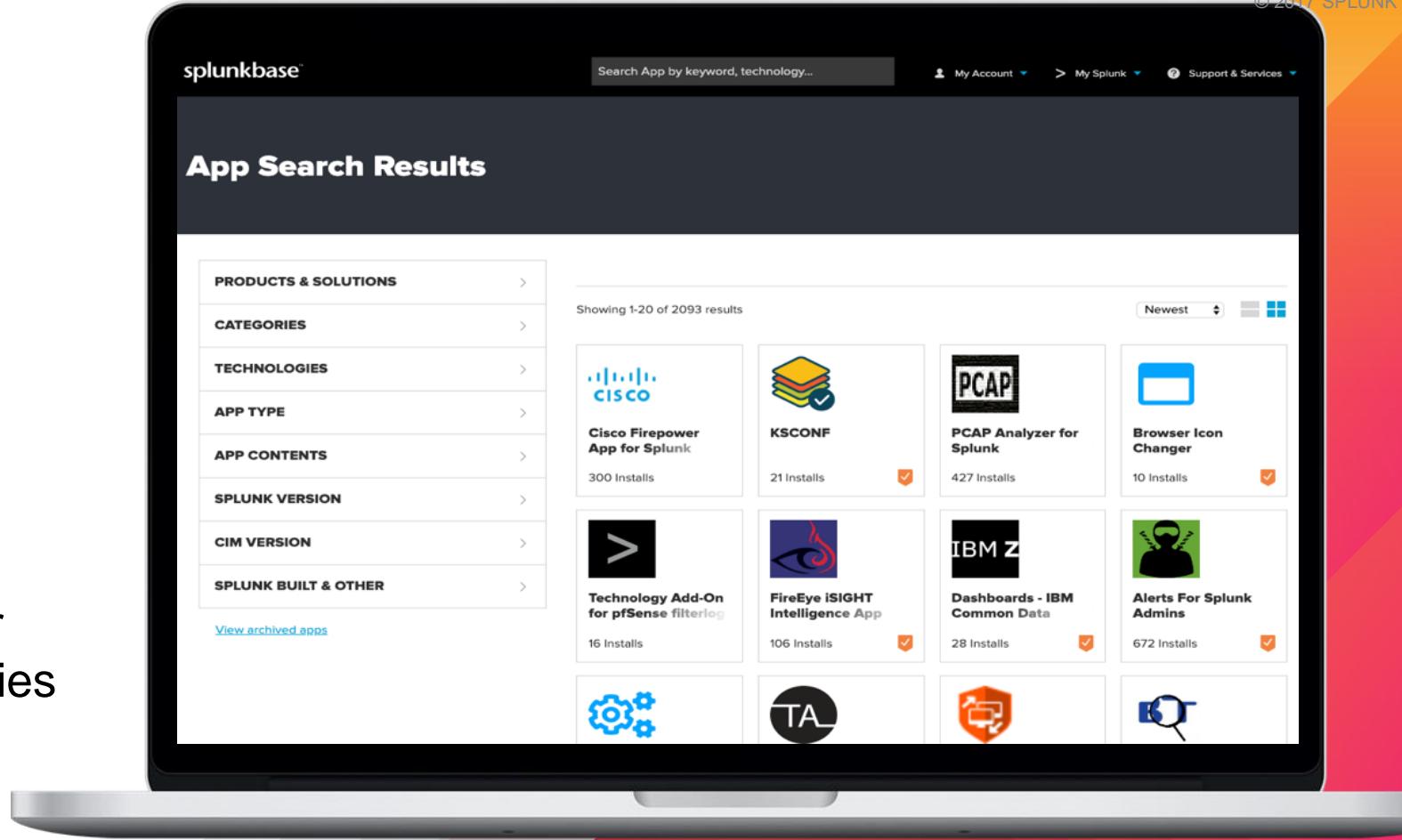
Education



Splunk Apps & Add-ons

<https://splunkbase.com>

- > 2000+ apps and add-ons
- > Pre-built searches, reports, visualisations and integrations for specific use cases and technologies
- > Download apps and customise them based on your requirements
- > Fast time to value from your data
- > Build and contribute your own apps!



Splunk Answers

<https://answers.splunk.com>

- > Get answers to your questions from Splunk 'know-it-all's, or share what you've learned to achieve know-it-all status yourself!

- > Engage with the Splunk community and learn how to get the most out of your Splunk deployment.

The image shows a smartphone displaying the Splunk Answers website. The top navigation bar includes links to Splunk.com, Documentation, Splunkbase, Answers, Wiki, Blogs, and Developers. The user profile 'pwest_splunk 20 • 1' is visible along with Logout and FAQ links. A search bar at the top right says 'Search Splunk Answers'. Below the header, there are two main sections: 'Find An Answer' (with a green checkmark icon) and 'Find Splunk Apps' (with a gear icon). The 'Find An Answer' section has a sub-section titled 'Recent Answers' with sorting options: newest, most voted, hottest, unanswered, and double points. It lists two recent posts: 'Duo Connector App does not update index on dashboard when a different index is configured' (by Duo Splunk Connector) and 'Insufficient permissions with Free license' (by Website input). The 'Find Splunk Apps' section features a card for 'Splunk Enterprise Security' which 'Quickly detect and respond to internal and external attacks.' A 'TRY IT NOW' button is shown. The 'Top Contributors' section shows profile pictures for two users.

Developer Resources

<http://dev.splunk.com>

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

The tablet screen shows the following content:

- splunk>dev**
- Welcome to the Splunk Developer Program**
- Build apps that Turn Data into Doing™ with Splunk.

Deliver apps and integrations that bring new kinds of data into the Splunk platform and deliver data-based insights, enabling users to investigate, monitor, analyze and act to make better and smarter decisions. Get started today.

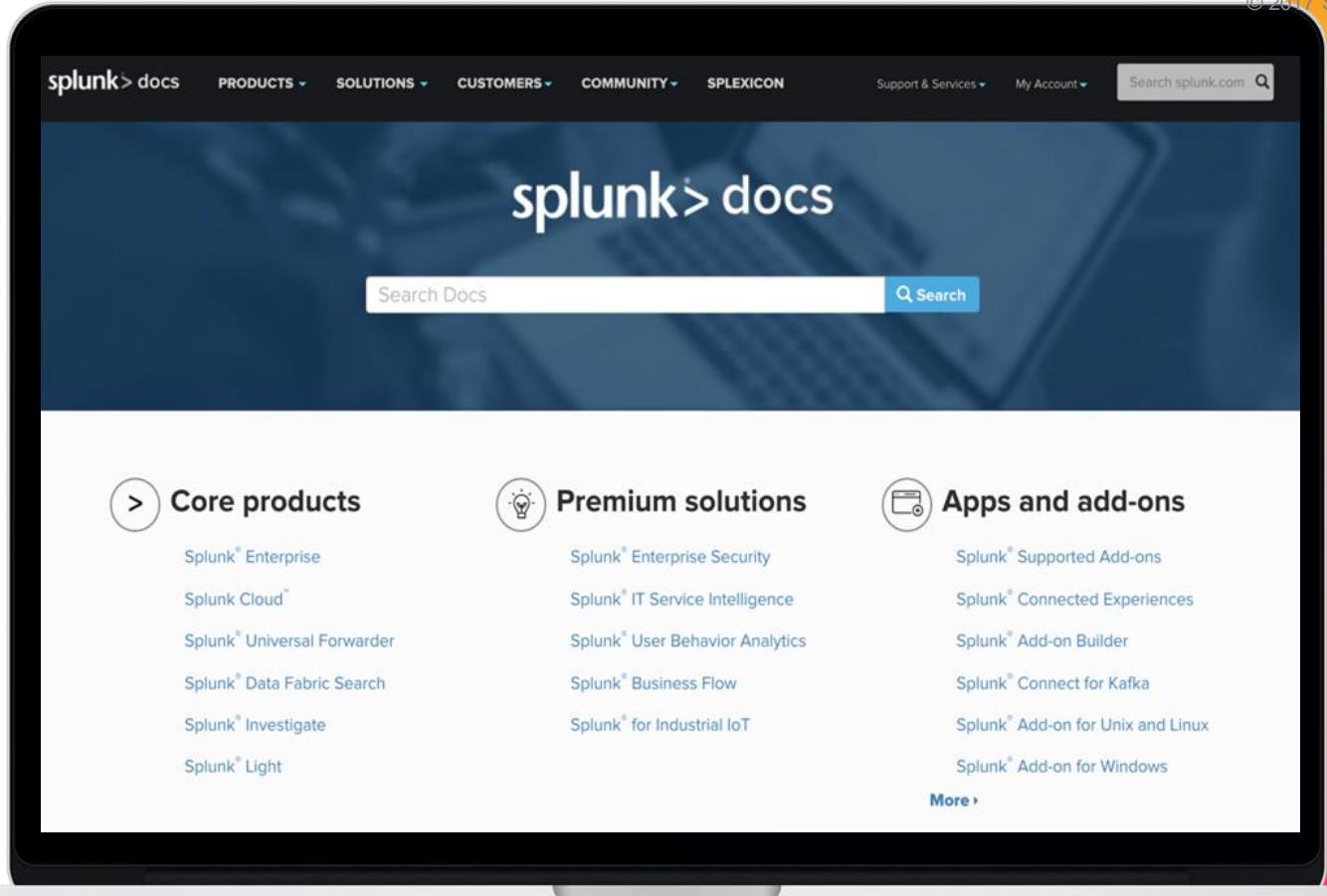
[Learn more](#)
- Featuring: Splunk Investigate**
- Splunk Investigate provides modern app-dev teams with a powerful, collaborative interface to easily investigate multiple data sources with reliable scalability and zero administration.

[Learn more >](#)
- A screenshot of the Splunk Investigate interface, showing a bar chart titled "SFO Airport Dashboard" with data for September 2018. The chart displays flight counts for various days of the month. Below the chart, key statistics are shown: Total Flights (984), On-time departures (893), Delayed departures (86.9), and Luggage arrival rate (80.3%).
- Develop for Splunk Enterprise** →
- Develop with Splunk Cloud Services** →

Documentation

<https://docs.splunk.com>

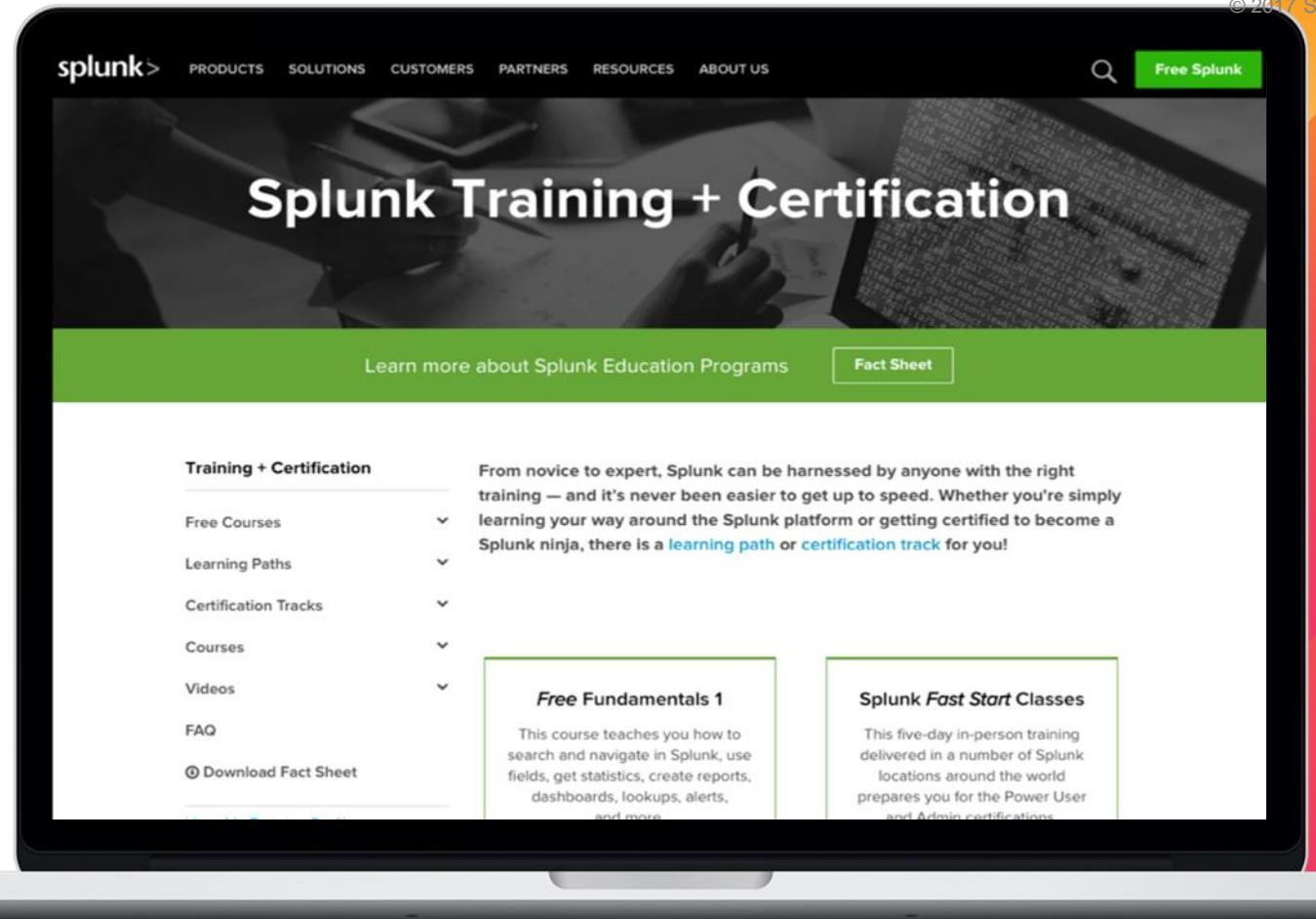
- > Splunk reference – Learn the commands!
- > Tutorials – Check out the search tutorial that even includes sample data to play with!
- > Use cases
- > References
- > Procedures/guides – installing, upgrading
- > And more!



Education

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

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



The image shows a smartphone displaying the Splunk Training + Certification website. The website has a dark header with the Splunk logo and navigation links for PRODUCTS, SOLUTIONS, CUSTOMERS, PARTNERS, RESOURCES, and ABOUT US. A search bar and a 'Free Splunk' button are also in the header. The main title 'Splunk Training + Certification' is displayed over a background image of hands working on a laptop keyboard. Below the title is a green button labeled 'Learn more about Splunk Education Programs' and a 'Fact Sheet' button. On the left, a sidebar titled 'Training + Certification' lists 'Free Courses', 'Learning Paths', 'Certification Tracks', 'Courses', 'Videos', and 'FAQ'. There is also a link to 'Download Fact Sheet'. To the right, there is descriptive text about Splunk's training options, mentioning 'Free Fundamentals 1' and 'Splunk Fast Start Classes'.

Splunk Training + Certification

Learn more about Splunk Education Programs Fact Sheet

Training + Certification

- Free Courses
- Learning Paths
- Certification Tracks
- Courses
- Videos
- FAQ

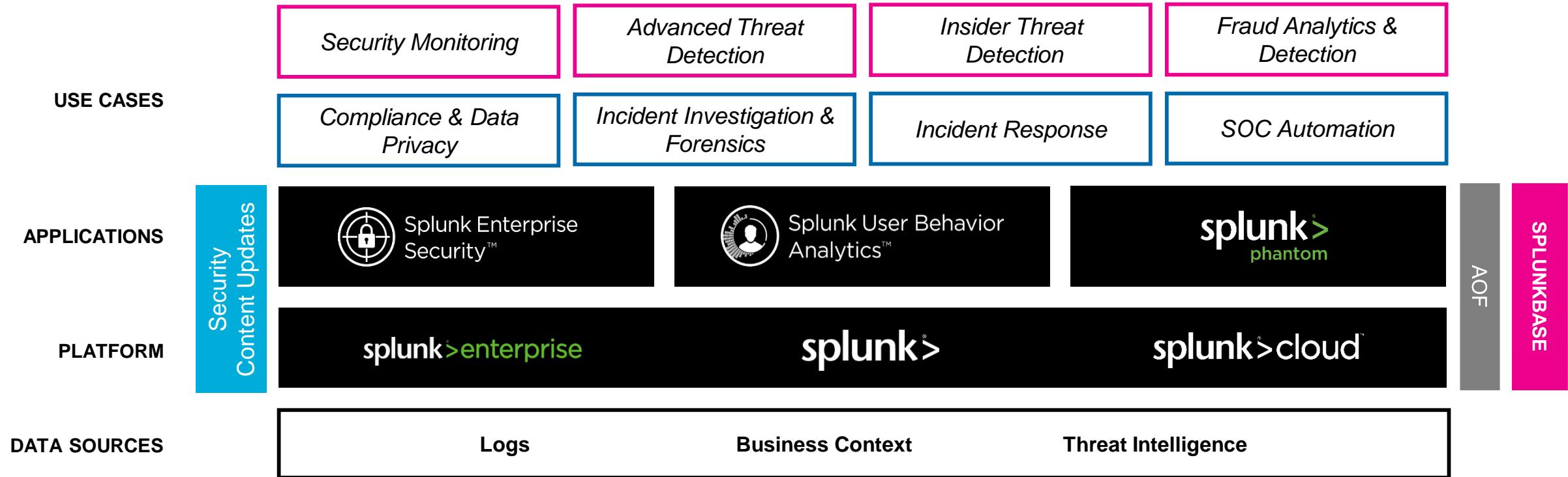
Download Fact Sheet

From novice to expert, Splunk can be harnessed by anyone with the right training — and it's never been easier to get up to speed. Whether you're simply learning your way around the Splunk platform or getting certified to become a Splunk ninja, there is a [learning path](#) or [certification track](#) for you!

Free Fundamentals 1
This course teaches you how to search and navigate in Splunk, use fields, get statistics, create reports, dashboards, lookups, alerts, and more.

Splunk Fast Start Classes
This five-day in-person training delivered in a number of Splunk locations around the world prepares you for the Power User and Admin certifications.

Security Operations Suite



Feedback

Just One More Thing



Thank You



splunk> turn data into doing™