splunk> .conf2017

Splunking to fight human trafficking

Sherrie Caltagirone | Global Emancipation Network
Monzy Merza | Head of Security Research
Satoshi Kawasaki | Splunk4Good Ninja

September 27th, 2017 | Washington, DC

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> .conf2017

Bio: Sherrie Caltagirone

Founder of Global Emancipation Network

Global Emancipation Network employs cutting-edge data analytics to disrupt human trafficking operations, embark on effective rescue campaigns, inform domestic and international policy, and restore the victims of modern-day slavery to dignity.

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Opera/9.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla"
ows NT 5.1: SV1: - .NET CLR 1.1.4322)" 468 125.17 14.10 "GET /product.screen?product_id=AV-CB-01&JSESSIONID=SD5SL4FF4ADFF7 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/..."
itemId=EST-16&product_id=RP-LI-02" [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://JSESSIONID=SD9SL4FF4ADFF7 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/..."
do?action=purchase-shopping_id=RP-LI-02" 468 125.17 14.10 "GET /product.screen?product_id=AV-CB-01&JSESSIONID=SD5SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product..."

splunk> .conf2017

Bio: Monzy Merza
Head of Security Research

▶ Splunker since 2011, Splunk customer before 2011

▶ Cyberisms, dev, test, eat, sleep, learn, and repeat

▶ Privileged to travel and learn from Splunk customers!

▶ Likes to speak at conferences with colleagues

▶ Doing 3 talks this year:

- *Day 2 Security Keynote Demo* with Maritza Perez

- *Splunking to fight human trafficking* with Satoshi Kawasaki

- *Threat Hunting with Machine Learning* with Phillipp Drieger
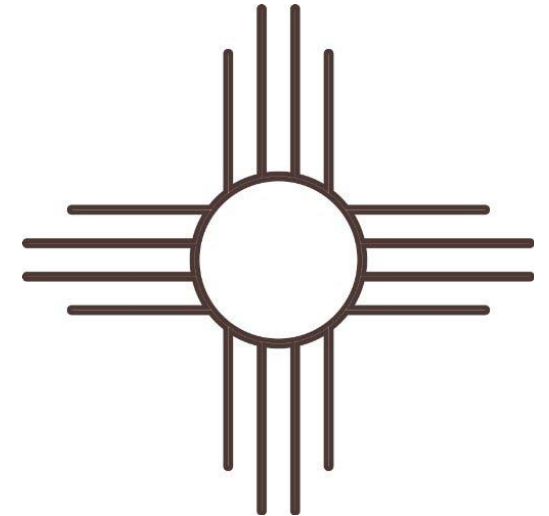
Thanks for coming to .conf and I'll be here all week! @monzymerza

splunk> .conf2017

Bio: Satoshi Kawasaki

Splunk4Good Ninja

BS in Aerospace Engineering from Georgia Tech

- ▶ Also joined Splunk in 2013
  - 3 years of Professional Services (PS)
  - 1+ year of Splunk4Good

- ▶ Unofficially became a dashboard/visualization specialist in PS
  - .conf 2014: *I Want that Cool Viz in Splunk!*
  - .conf 2015: *Enhancing Dashboards with JavaScript!*

- ▶ Also doing 3 talks this year
  - .conf 2017: *Speed up your searches!*
  - .conf 2017: *Splunking to fight human trafficking*
  - .conf 2017: *Splunking the 2016 presidential election*

hobbes3

You are here.

splunk> .conf2017

"**Enslave** the liberty of but one human being and the liberties of the world are put in peril."

—*William Lloyd Garrison,*
19th century abolitionist

Types of human trafficking

- ▶ Sex trafficking
- ▶ Forced labor
- ▶ Debt bondage
- ▶ Domestic servitude
- ▶ Child soldiering
- ▶ Mail-order brides
- ▶ Forced begging
- ▶ Child sex tourism
- ▶ and others

Agenda

- Major pain points in the anti-trafficking community
- Data-led, intelligence-centric approach
- Architecture and components of the analysis system
- Lessons and next steps

Global trafficking statistics

From "Trafficking in Persons Report 2017" – U.S. Department of State

Year	Prosecutions	Convictions	Victims identified	New or amended legislation
2009	5,606 (432)	4,166 (335)	49,105	33
2010	6,017 (607)	3,619 (237)	33,113	17
2011	7,909 (456)	3,969 (278)	42,291 (15,205)	15
2012	7,705 (1,153)	4,746 (518)	46,570 (17,368)	21
2013	9,460 (1,199)	5,776 (470)	44,758 (10,603)	58
2014	10,051 (418)	4,443 (216)	44,462 (11,438)	20
2015	19,127 (857)	6,615 (456)	77,823 (14,262)	30
2016	14,897 (1,038)	9,071 (717)	66,520 (17,465)	35

The numbers in parentheses are those of labor trafficking prosecutions, convictions, and victims identified.

splunk> .conf2017

Many silos

list of organizations against human trafficking

All · News · Images · Videos · Shopping · More · Search tools

About 1,080,000 results (0.64 seconds)

Stop Human Trafficking - No More Slavery - rickymartinfoundation.org
Ad www.rickymartinfoundation.org/Stop_Human/Trafficking ▾
We denounce **human trafficking** and educate about its existence.

Fight Human Trafficking - Anti-Trafficking Aid Organization
Ad www.compassion.com/Human-Trafficking ▾
See the Facts. Learn How to Help.

Fight Human Trafficking - destinyrescue.org
Ad www.destinyrescue.org/ ▾
Children in **Human Trafficking** Need Rescuing. Join The Fight!
Donate to Destiny Rescue · About Destiny Rescue · Fund A Project · Sponsor A Child

Stop Human Trafficking - Help Us Stop This Sickening Crime
Ad www.orphansecure.com/ ▾
We Are Preserving Human Rights.
Protecting Children · Non-Profit · Freedom App · Anti-Human Trafficking
What We Do · Contact Us · Freedom App · Who Are We?

List of organizations that combat human trafficking - Wikipedia, the free ...
https://en.wikipedia.org/.../List_of_organizations_that_combat_human_traf... ▾ Wikipedia ▾
This is a **list of organizations** with a primary, or significant, commitment to ending human ... Awareness
Against Human Trafficking (HAART) is non-governmental **organization** fighting **against human
trafficking** in Kenya. Bishop Outreach, a ...

International Organizations - HumanTrafficking.org
www.**humantrafficking**.org/countries/united_states_of_america/international_orgs ▾

List of organizations that combat human trafficking | Open Access ...
research.omicsgroup.org/index.../List_of_organizations_that_combat_human_traffick... ▾
This is a **list of organisations** with a primary, or significant, commitment to ending human ... Awareness
Against Human Trafficking (HAART) is non-governmental ...

Connect | List of Antislavery Organizations - End Slavery Now
www.endslaverynow.org/connect ▾
Antislavery Directory. **Organizations** where you can get involved in the fight **against** modern-day
slavery and **human trafficking**.

List of organizations that combat human trafficking

From Wikipedia, the free encyclopedia

This is a dynamic list and may never be able to satisfy particular standards for completeness. You can help by expanding it with reliably sourced entries.

This is a list of organizations with a primary, or significant, commitment to ending human trafficking.

Other lists include:

- Freedom Collaborative, which is managed by Liberty Asia.
- http://www.globalmodernslavery.org/

List   [edit]

- Anti-Slavery International, Anti-Slavery International works at local, national and international levels to eliminate all forms of slavery around the world
- 8th Day Center for Justice, a Roman Catholic non-profit organization based in Chicago, Illinois
- A Better World, an organization that is based in Lacombe, Alberta, Canada[1]
- A21 Campaign, a 501(c)(3) non-profit, non-governmental organization that works to fight human trafficking
- ACT Alberta, a Canadian coalition of Government of Alberta representatives, non-governmental organizations, community organisations, and the Royal Canadian Mounted Police[2]
- Agape International Missions, a nonprofit organization in Cambodia[3]
- Arizona League to End Regional Trafficking, a coalition representing partnerships with law enforcement, faith-based communities, non-profit organizations, social service agencies, attorneys and concerned citizens.
- Awareness Against Human Trafficking (HAART) is non-governmental organization fighting against human trafficking in Kenya.
- Bishop Outreach, a non-profit, non-governmental organization involved in rescuing those enslaved in human trafficking.
- Breaking Free, a nonprofit organization[4] based in Saint Paul, Minnesota, United States that provides various services to prostitutes, such as help finding a place to live and a job outside the sex industry[5]
- California Against Slavery, a human rights organization directed at strengthening California state laws to protect victims of sex trafficking
- Centre to End All Sexual Exploitation, a nonprofit organization that helps human trafficking victims, sex workers, and the homeless by providing them with resources[6]
- Coalition to Abolish Slavery and Trafficking, a nonprofit organization that helps human trafficking victims by providing Social Services, Legal Services, and Outreach and Training
- Chab Dai, a coalition founded by Helen Sworn[7] that connects Christian organizations committed to ending sexual abuse and trafficking.[8][9]
- Coalition Against Trafficking in Women, an international non-governmental organization opposing human trafficking, prostitution, and other forms of commercial sex
- Coalition to Abolish Slavery and Trafficking, a Los Angeles-based anti-human trafficking organization
- Deborah's Gate, a human trafficking victims safe house run by The Salvation Army in Vancouver, British Columbia, Canada that opened in 2009[10]
- Devatop Centre for Africa Development, a nonprofit organization in Nigeria with focus on combating human trafficking, gender-based violence, child abuse; and providing educational supports to vulnerable children.
- Durbar Mahila Samanwaya Committee, a collective of 65,000 sex workers in West Bengal
- ECPAT, an international non-governmental organisation and network headquartered in Thailand which is designed to end the commercial sexual exploitation of children
- The Emancipation Network, an international organization dedicated to fighting human trafficking and modern-day slavery
- EVE, an advocacy group based in Vancouver, British Columbia, Canada[11]
- The Exodus Road, a non-profit coalition of organizations specialized in the intervention component of human trafficking, training and funding partnerships with local authorities to actively rescue people trapped in human States.
- Face to Face Bulgaria, an organization whose primary mission is to prevent cases of forced prostitution and human trafficking in Bulgaria[12][13]
- Florida Abolitionist, a nonprofit,[14] non-governmental organization opposing human trafficking in Florida, United States
- Free the Slaves, is dedicating to ending Slavery Worldwide
- Freeset, an organization whose primary mission is to provide sustainable employment and economic empowerment to victims of sex trafficking in South Asia.

Anti-trafficking stakeholders
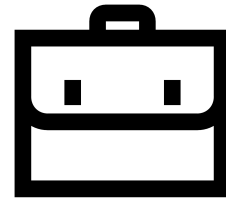
Who owns the data?
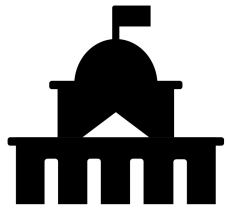
Government
- Government Agencies
- Law Enforcement
- Justice System
- Legislators
- International Organizations

Nonprofits
- Anti-trafficking Organizations
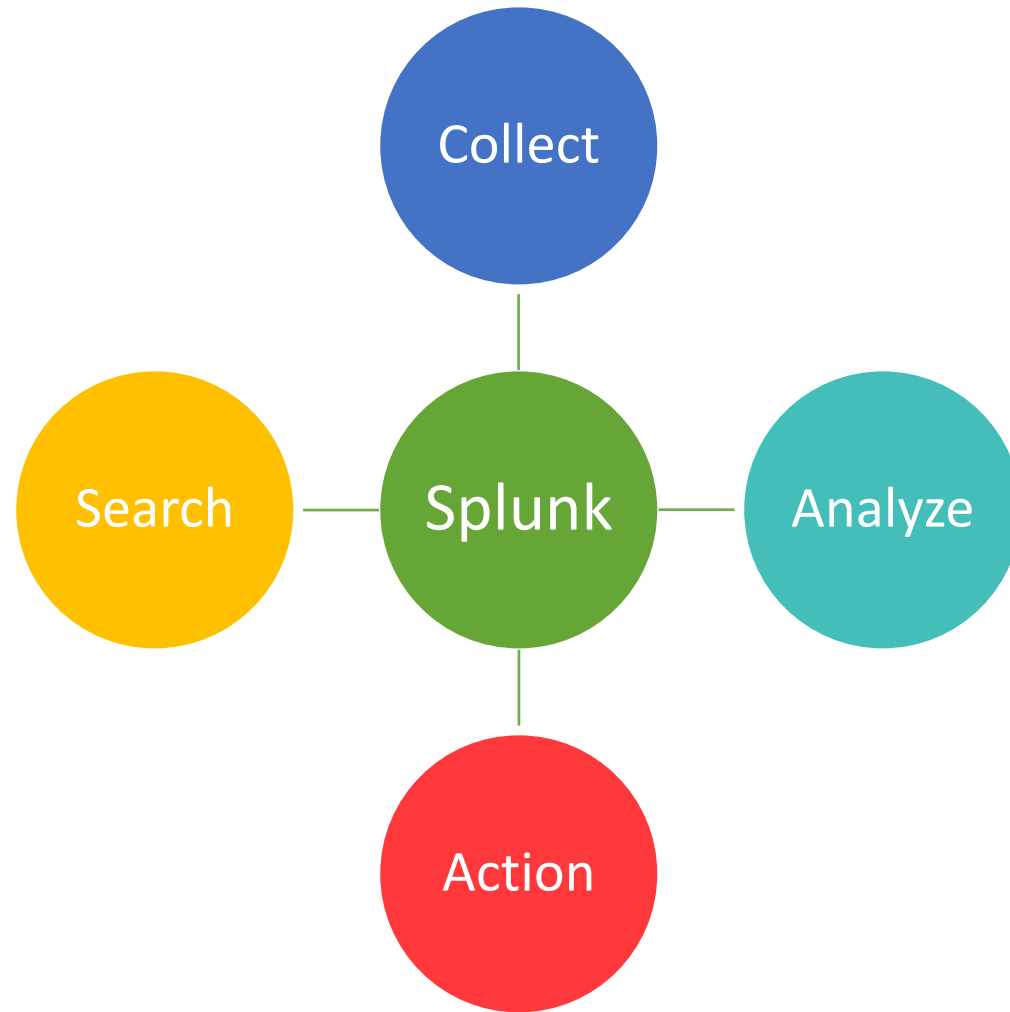- Victim Services
- Hotline Operators
- Academics

Private
- Private Businesses
- Healthcare Providers

splunk> .conf2017

GEN's anti-trafficking ecosystem

GLOBAL EMANCIPATION NETWORK

Data
- Minerva
- Secure data sharing
- Analytics

Exchange
- Deconfliction
- Best Practices
- Efficient VSP identification

Tech
- Resource-sharing
- Tech Dispersion
- Tech volunteers

splunk> .conf2017

Simplified process

Collect

Splunk

Search

Analyze

Action

Collect

- Recorded Future scrapes based on keywords
- Full ads are pulled down via Backpage API
- Custom scrappers pull forum posts from other relevant forum boards
- Splunk indexes the posts and its metadata

splunk> .conf2017

Example data

```
>    4/11/17           { [-]
     12:00:36.000 PM        collection_time: 2017-04-10T22:41:38.809790+00:00
                            collector_function: XXXXX_scraper
                            collector_org: ncsu
                            creation_date: 2017-04-07T13:11:00+00:00
                            data_definition: textpostmetadata
                            data_definition_version: 1
                            forum_title: OR Provider Posts
                            forum_url: https://www.XXXXX.com/forumdisplay.php?116-OR-Provider-Posts
                            id: zVsS_Ajf9DO
                            imageArchiveLinks: [ [+]
                            ]
                            imageLinks: [ [+]
                            ]
                            imageSHA256Hashes: [ [+]
                            ]
                            internalLocation: https://genarchive.blob.core.windows.net/htmlarchive/XXXXX/zVsS_Ajf9DO.html
                            last_update_date: null
                            location: portland
                            md5: c69892f16bf3923a73bd328168d3ab32
                            originalLocation: https://www.XXXXX.com/showthread.php?9999&p=1111&mode=threaded#post22222
                            post_type: ad
                            rating: 0 / 5
                            raw: { [-]
                              body_text: Service Type:
                                  Escort
                          Come see me. South east Portland.
                        🐦 Finally back!!! 🎉✨Incall today only! 🐦Sandy blvd✨🎉
                        I really want some company  I got a new number 555_threefoureight_2432
                        No blocked numbers! Serious men only please.


                            }
                            reply_count: 1077
                            reply_parent_id: 9212988
                            security: { [+]
                            }
                            self_id: 9212988
                            sha1: e10c577f1e1e35999802ae08e42641269a1ac2e8
```

Example data challenges

Post date

Unpredictable length of post

Mixed fonts and formats

4/11/17
12:00:36.000 PM

```
{ [-]
     collection_time: 2017-04-10T22:41:38.809790+00:00
     collector_function: XXXXX_scraper
     collector_org: ncsu
     creation_date: 2017-04-07T13:11:00+00:00
     data_definition: textpostmetadata
     data_definition_version: 1
     forum_title: OR Provider Posts
     forum_url: https://www.XXXXX.com/forumdisplay.php?116-OR-Provider-Posts
     id: zVsS_Ajf9DO
     imageArchiveLinks: [ [+]
     ]
     imageLinks: [ [+]
     ]
     imageSHA256Hashes: [ [+]
     ]
     internalLocation: https://genarchive.blob.core.windows.net/htmlarchive/XXXXX/zVsS_Ajf9DO.html
     last_update_date: null
     location: portland
     md5: c69892f16bf3923a73bd328168d3ab32
     originalLocation: https://www.XXXXX.com/showthread.php?9999&p=1111&mode=threaded#post22222
     post_type: ad
     rating: 0 / 5
     raw: { [-]
       body_text: Service Type:
            Escort
     Come see me. South east Portland.
  💋 Finally back!!! 🎉✨Incall today only! 💋Sandy blvd✨🎉
  I really want some company  I got a new number 555_threefoureight_2432
  No blocked numbers! Serious men only please.


       }
     reply_count: 1077
     reply_parent_id: 9212988
     security: { [+]
     }
     self_id: 9212988
     sha1: e10c577f1e1e35999802ae08e42641269a1ac2e8
```

Search

- Search any posts on any keywords
- Extract new fields from the raw text

Searching

New Search

```
index=main sourcetype=mscs:storage:blob data_definition=textpostmetadata post_type=ad
| rex field=forum_title "^(?<state>[A-Z]{2}) "
```

✓ 712 events (4/11/17 12:00:00.000 AM to 4/13/17 12:00:00.000 AM)   No Event Sampling ⌄   Job ⌄   ‖   ■

| Events (712) | Patterns | Statistics | Visualization |

Format Timeline ⌄   — Zoom Out   + Zoom to Selection   × Deselect
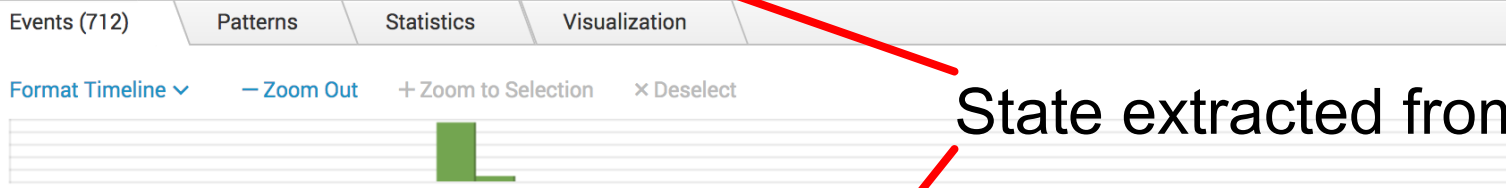
State extracted from another field

List ⌄   ✎ Format   20 Per Page ⌄   ‹ Prev 1 2 3 4

‹ Hide Fields	≡ All Fields

i	Time	Event
›	4/11/17 12:00:38.000 PM	{ [-] collection_time: 2017-04-10T22:12:56.790515+00:00 collector_function: XXXXX scraper

Selected Fields
- *a* host 1
- *a* source 100+
- *a* sourcetype 1

Interesting Fields
- *a* collection_time 100+
- *a* collector_function 1
- *a* collector_org 1
- *a* creation_date 100+
- *a* data_definition 1
- # data_definition_version 1
- *a* forum_title 16
- *a* forum_url 16
- *a* id 100+

forum_title   ✕

16 Values, 99.86% of events   Selected   Yes   No

Reports

Top values   Top values by time   Rare values

Events with this field

Top 10 Values   Count   %

	Count	%	
WA Provider Posts	306	43.038%	▬
OR Provider Posts	177	24.894%	▬
WA LMA & LMS	72	10.126%	▮

Disruption

Los Angeles Times

JANUARY 9, 2017, 10:10 PM

Backpage shuts down adult section, citing government pressure and unlawful censorship campaign

Ad creation on alternative site

splunk> .conf2017

Analyze

- Single value panels for overviews
- Visualizations for easier interpretations
- Interactive inputs and drilldowns for investigations and filtering

splunk> .conf2017

Dashboards

Interactive filters for further investigations

Dashboards

Top 50 users by # of posts

| 2009 | 2010 | 2011 | April 18 | 2013 | 2014 | 2015 | 2016 | 2017 |

32.00

1.00

2.00

0.00

0.00

0.00

5.00

10.00

1.00

1.00

0.00

0.00

7.00

splunk> .conf2017

Dashboards

User info (sorted by # of posts)

Drilldown to "User Details" dashboard

user_name ⇅	user_id ⇅	posts ⇅	phone ^	email ⇅	location ⇅
▓▓▓▓	107051	97	139502▓	clair▓▓@gmail.com	everett
▓▓▓▓	96929	1	140685▓ 206259▓ 206312▓ 206400▓ 206451▓ 206639▓	N/A	renton
▓▓▓	118015	1	142075▓ 360515▓	N/A	portland
▓▓▓	105833	10	143086▓ 206289▓	N/A	everett statewide
▓▓▓▓	187444	1	202753▓ 253881▓	shay▓▓@yahoo.com shay▓▓@yahoo.com	dt seattle olympia tacoma
▓▓▓▓	191991	1	202810▓	N/A	s. seattle
▓▓▓	242712	2	203427▓	N/A	dt seattle kent tacoma
▓▓▓	126069	2	206200▓	N/A	beaverton bellevue bellingham b
▓▓▓	209219	8	206201▓ 425615▓	N/A	portland s. seattle seattle

Numbers, emails, and locations tied to username

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=FL-SW-01" "Opera/9...
128.241.220.82 - - [07/Jan 18:10:56:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=GIFTS..."
317 27.160.0.0 - .NET CLR 1.1.4322) "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD1BSL8FF2ADFF9..."
itemId=EST-16&product_id=RP-LI-02" 468 125.17 14 106] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL5FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping..."

splunk> .conf2017

Drilldown
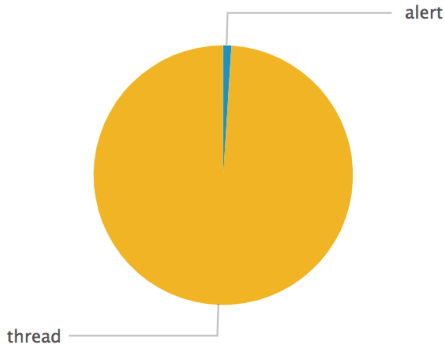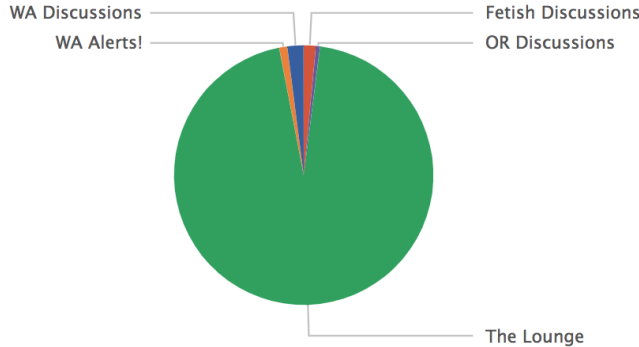
Drilling down to a single user
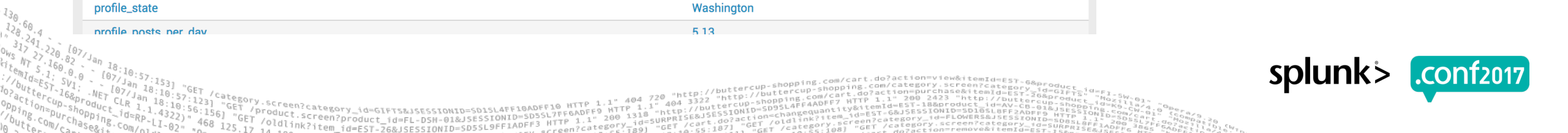
Action

- Alerts are based on thresholds for analytics
- Can be adhoc – e.g. alert on a keyword – or more complex analytics
- Alerts can drive actions – emails, scripts, API calls

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product...
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product...
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://JSESSIONID=SD95L4FF4ADFF7 HTTP 1.1" 200 2423 "http://buttercup-shopping...
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.100

splunk> .conf2017

The Splunk solution
A data-led, intelligence-centric solution

Operational constraints

- ▶ Limited budget
- ▶ Time to value
- ▶ Non-technical investigators
- ▶ Multiple access levels and enrichment layers

Splunk solution

- ▶ Reduces ingest and parsing costs
- ▶ Imbedded analytics speeds process
- ▶ Easy-to-use dashboards and UI skins
- ▶ Central nerve center

What's next and call to action!

▶ Integrate with image processing and other databases

▶ Natural language processing

▶ Enable 3rd parties to interact/grow the system

▶ Full time developer and committed volunteers needed – please donate!

▶ Follow Us – Global Emancipation Network!

- @GblEmancipation

- www.globalemancipation.ngo

Thanks to our partners
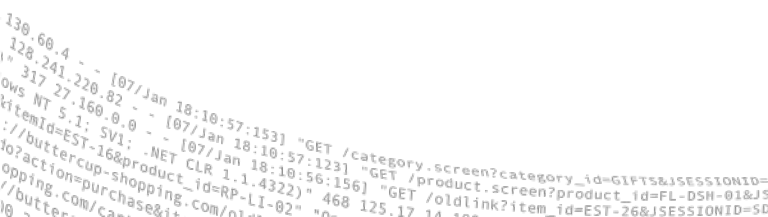

This work is being made possible with support from Splunk management, the Splunk4Good project, and the expert help of partners in support of the Global Emancipation Network. Thank you!!

splunk> .conf2017

© 2017 SPLUNK INC.

Thank You

Don't forget to rate this session in the .conf2017 mobile app

splunk> .conf2017