

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.

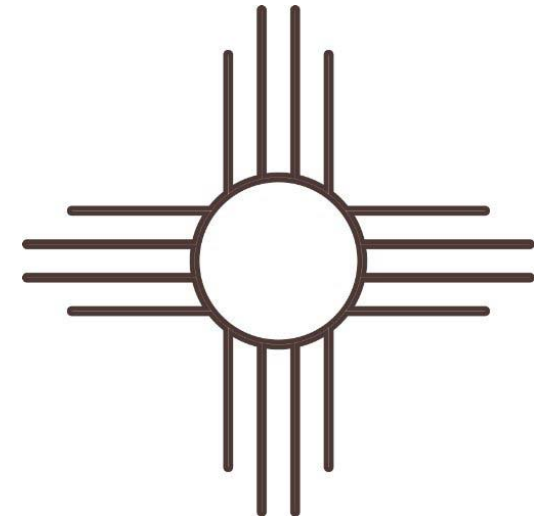
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements 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, 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. © 2017 Splunk Inc. All rights reserved.

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

130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Opera/9.80 (Win
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/4.0 (Compaq i486)
ows NT 5.1; SV1; - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03" "Opera/9.80 (Win
item_id=EST-16&product_id=RP-LI-02" 468 125.17 14 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Opera/9.80 (Win
ofaction=purchase&itemId=EST-26&product_id=FI-SW-03" 468 125.17 14 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Opera/9.80 (Win
opping.com/purchase&itemId=EST-26&product_id=FI-SW-03" 468 125.17 14 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Opera/9.80 (Win

"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.

List of organizations that combat human trafficking

*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.*

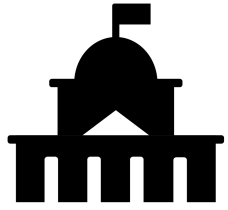
Other lists include:

- 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 trafficking in [United States](#).
- [Face to Face Bulgaria](#), an organization whose primary mission is to prevent cases of forced prostitution and [human trafficking](#) in [Bulgaria](#)^{[12][13]</}

Anti-trafficking stakeholders

Who owns the data?



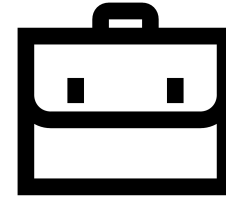
Government

- Government Agencies
- Law Enforcement
- Justice System
- Legislators
- International Organizations



Nonprofits

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



Private

- Private Businesses
- Healthcare Providers

GEN's anti-trafficking ecosystem



Data

- Minerva
- Secure data sharing
- Analytics

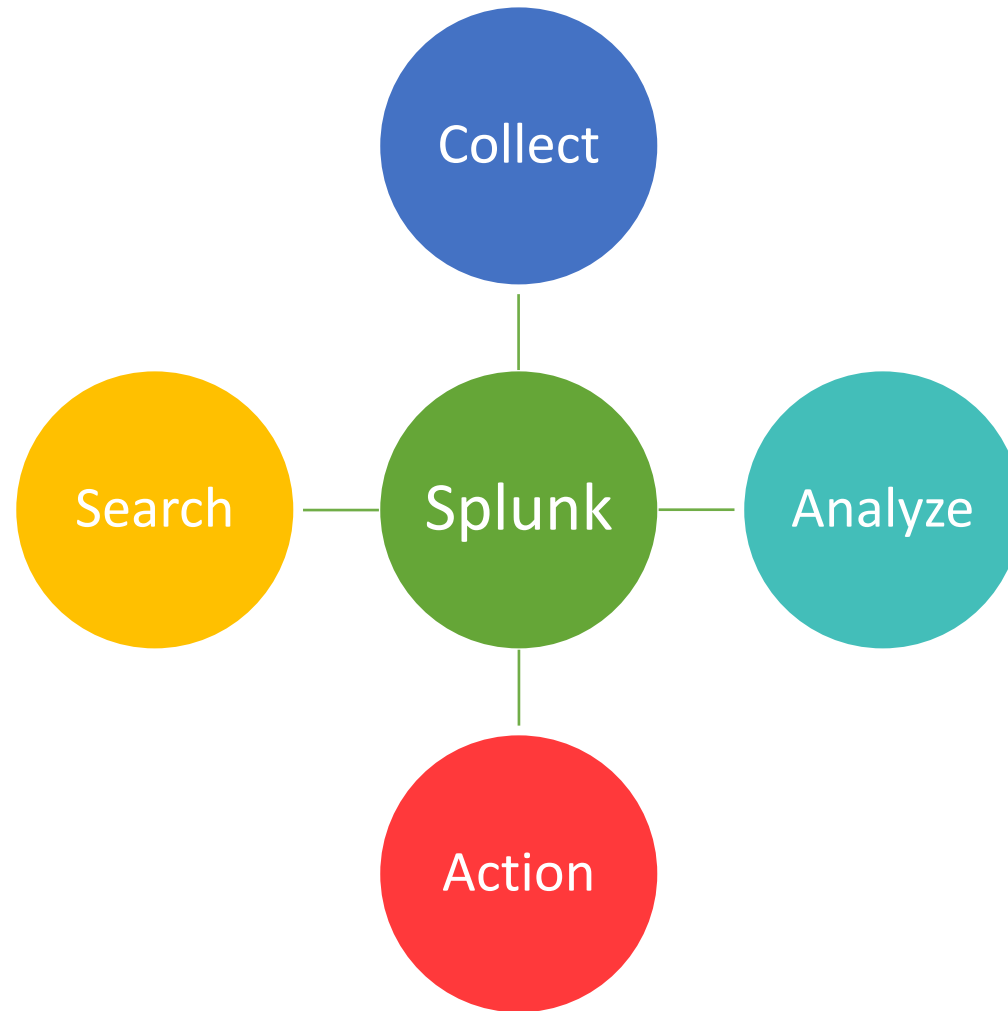
Exchange

- Deconfliction
- Best Practices
- Efficient VSP identification

Tech

- Resource-sharing
- Tech Dispersion
- Tech volunteers

Simplified process



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

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_Ajf9D0
imageArchiveLinks: [ [+]
]
imageLinks: [ [+]
]
imageSHA256Hashes: [ [+]
]
internalLocation: https://genarchive.blob.core.windows.net/htmlarchive/XXXXX/zVsS_Ajf9D0.html
last_update_date: null
location: portland
md5: c69892f16bf3923a73bd328168d3ab32
originalLocation: https://www.XXXXX.com/showthread.php?9999&p=1111&mode=threaded#post2222
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_threefouright_2432
    No blocked numbers! Serious men only please.
  }
reply_count: 1077
reply_parent_id: 9212988
security: { [+]
}
self_id: 9212988
sha1: a10c577f1e1e35999802ae08e47641769a1ac2e8
```


Searching

Q 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

List ▾ Format 20 Per Page ▾ < Prev 1 2 3 4

< Hide Fields All Fields

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+

Time Event

4/11/17 12:00:38.000 PM { [-]
collection_time: 2017-04-10T22:12:56.790515+00:00
collector_function: XXXXX_scraner

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

State extracted from another field

Disruption

Los Angeles Times

JANUARY 9, 2017, 10:10 PM

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



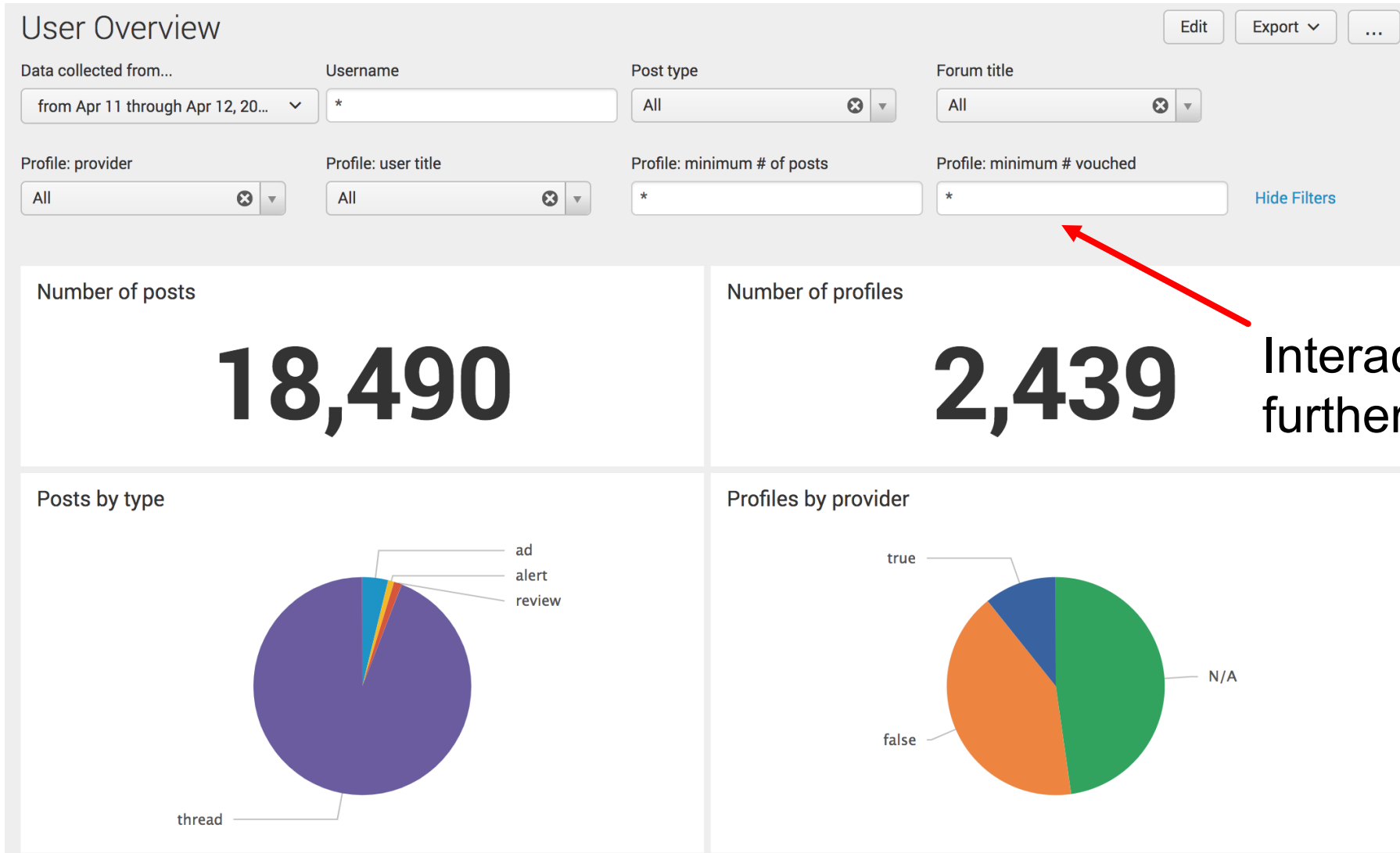
Ad creation on
alternative site



Analyze

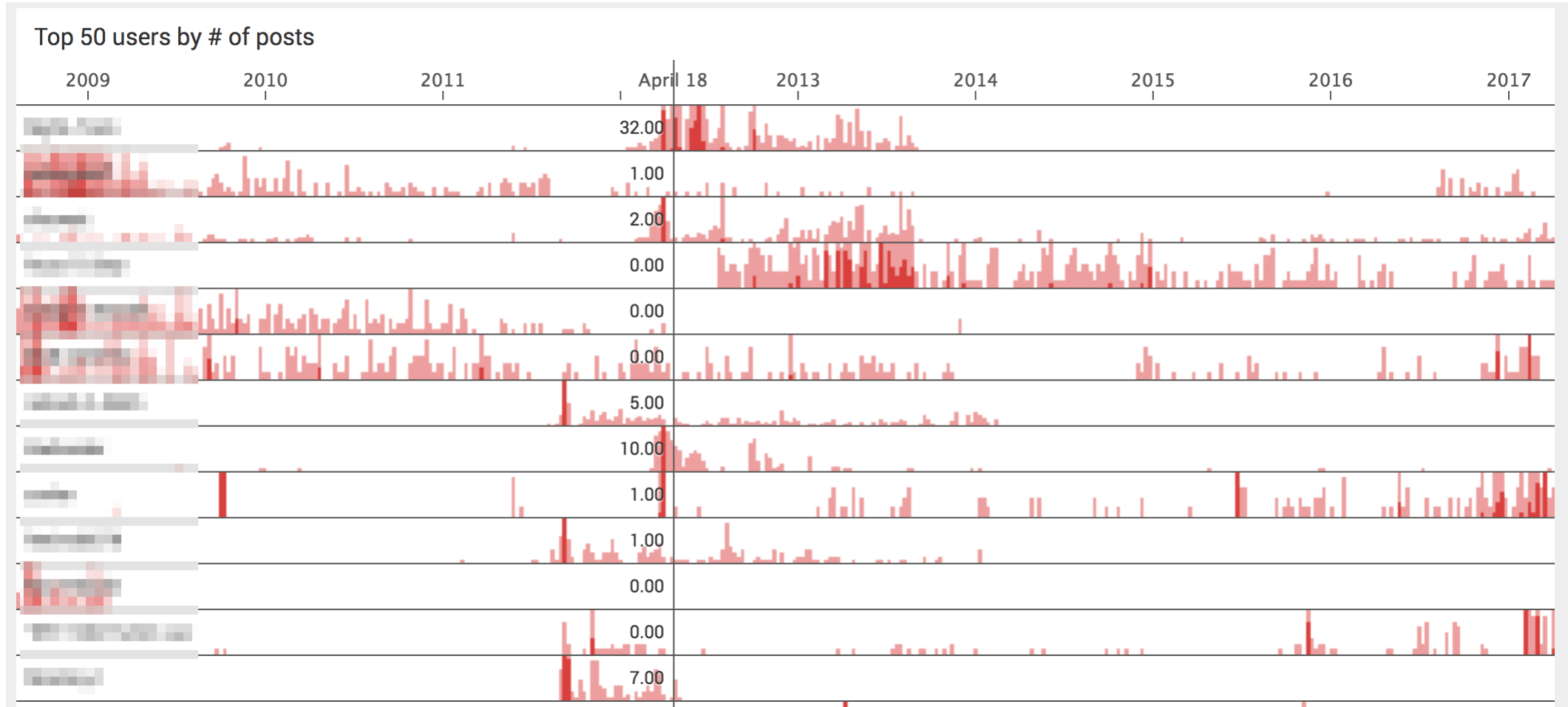
- Single value panels for overviews
- Visualizations for easier interpretations
- Interactive inputs and drilldowns for investigations and filtering

Dashboards



Interactive filters for further investigations

Dashboards



Dashboards

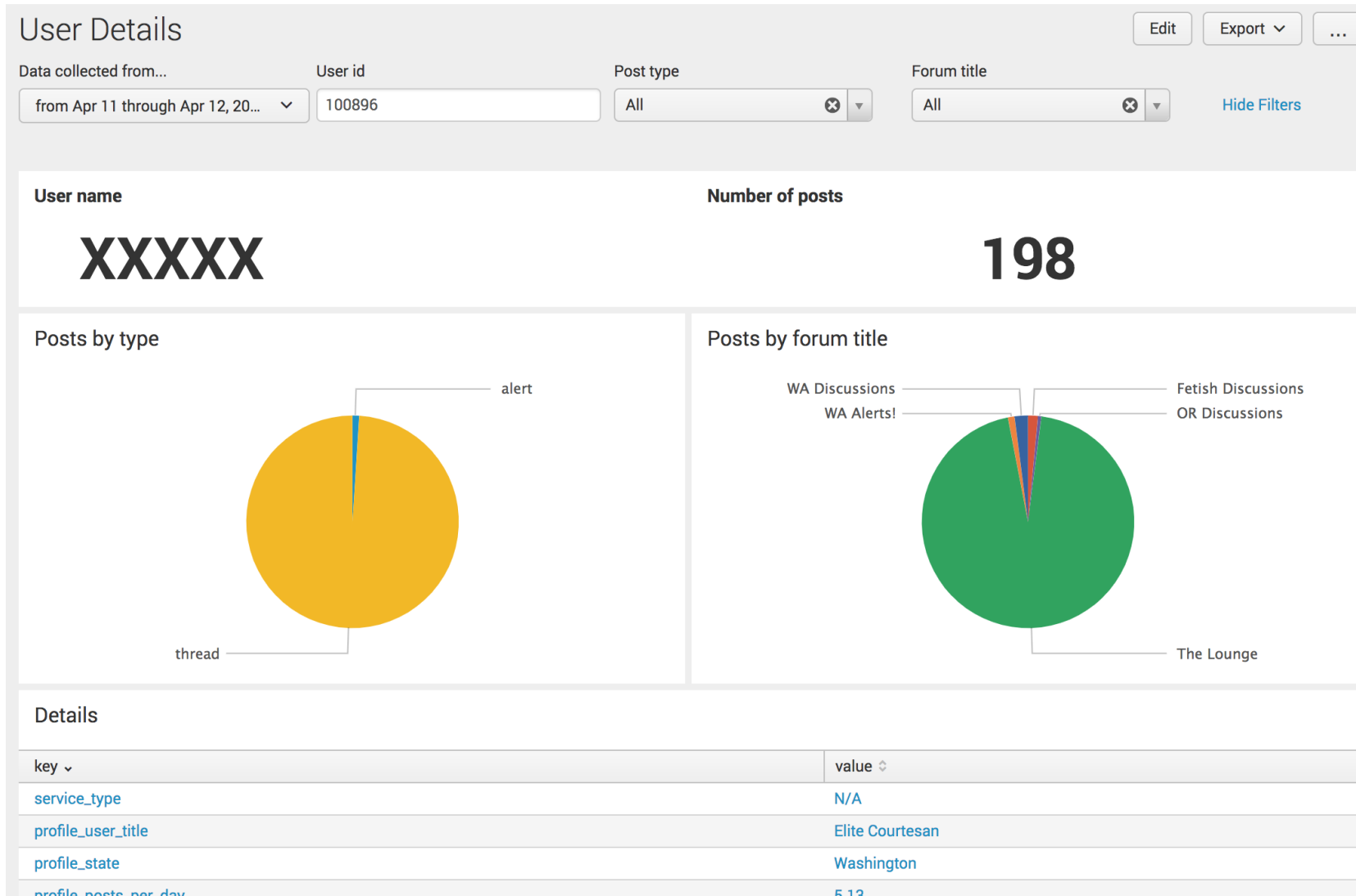
User info (sorted by # of posts)

Drilldown to "User Details" dashboard

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

Numbers, emails, and locations tied to username

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

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

- ▶ 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



Recorded Future

neustar™



Microsoft

Philanthropies



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

Thank You

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

splunk> .conf2017