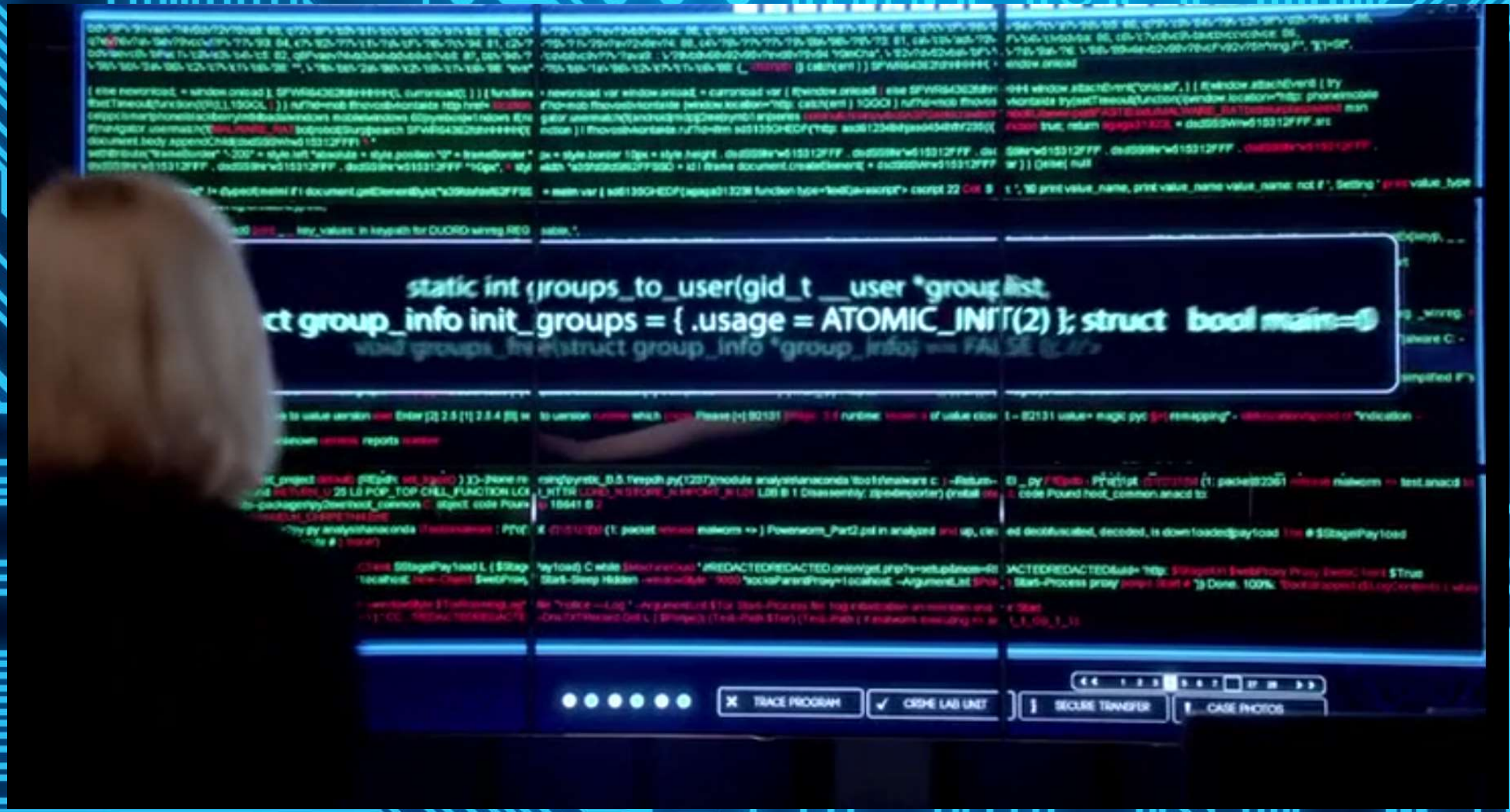
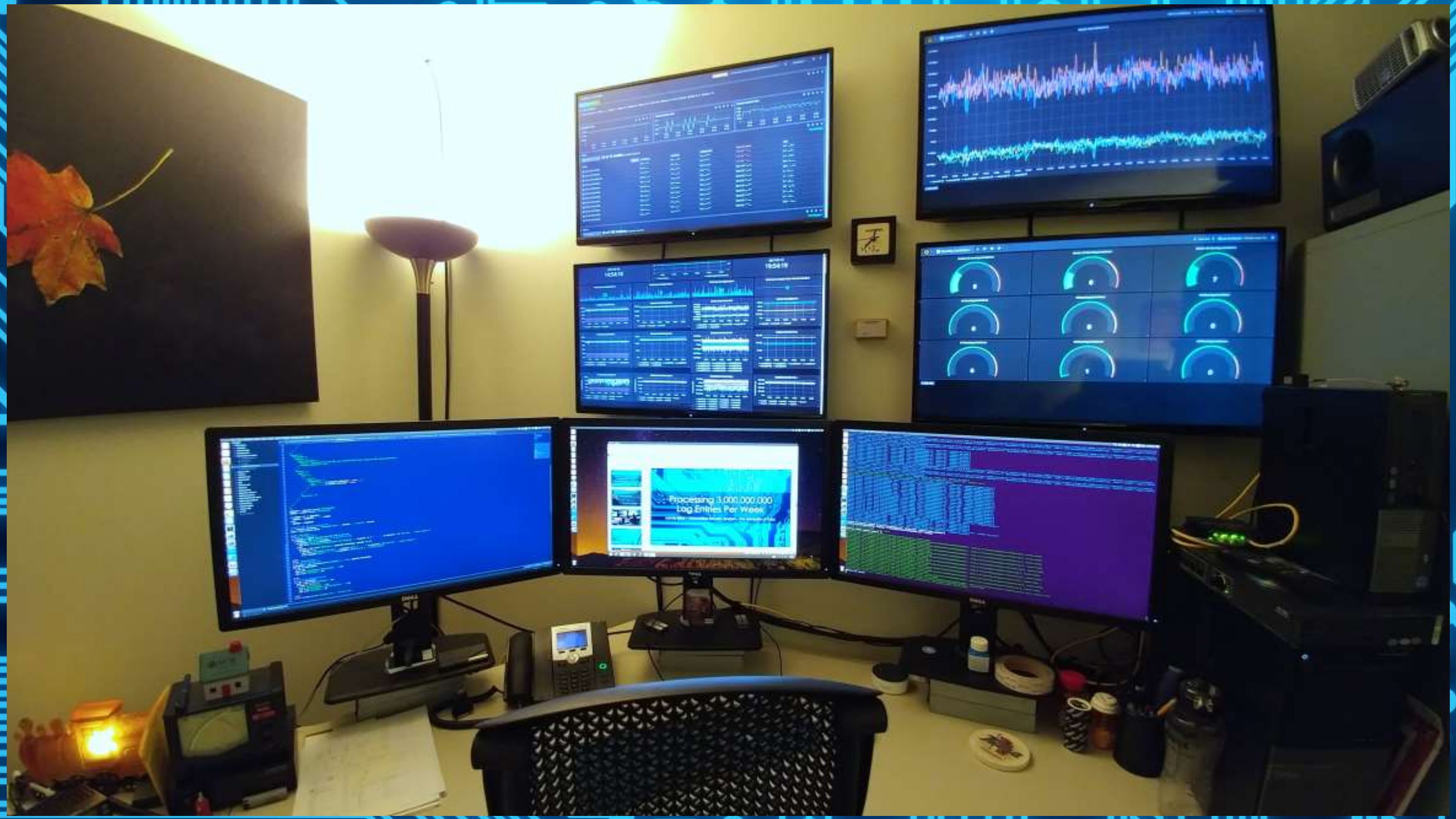
Processing 3,000,000,000 Log Entries Per Week

Landy Bible – Information Security Analyst – The University of Tulsa


static int groups_to_user(gid_t __user *group_list,
ct group_info init_groups = { .usage = ATOMIC_INI(2) }; struct
bool main
TRACE PROGRAM
CRIME LAB UNIT
SECURE TRANSFER
CASE PHOTOS


Processing 3,000,000,000
Log Entries Per Week

THE UNIVERSITY of TULSA


@ljb2of3
GitHub repo has slides and setup guide

It's All About The Data

What is the interesting data?

How do you collect it?

How do you search it?

What is the data?

What are the questions?

- How many computers are active on the network?
- How many connections does our email server get?
- Which countries are our servers connecting to?
- Are there any computers running port scans?
- Which computers are sending emails?
- What computer was assigned a particular IP address?
- On which ports are our servers accepting connections?

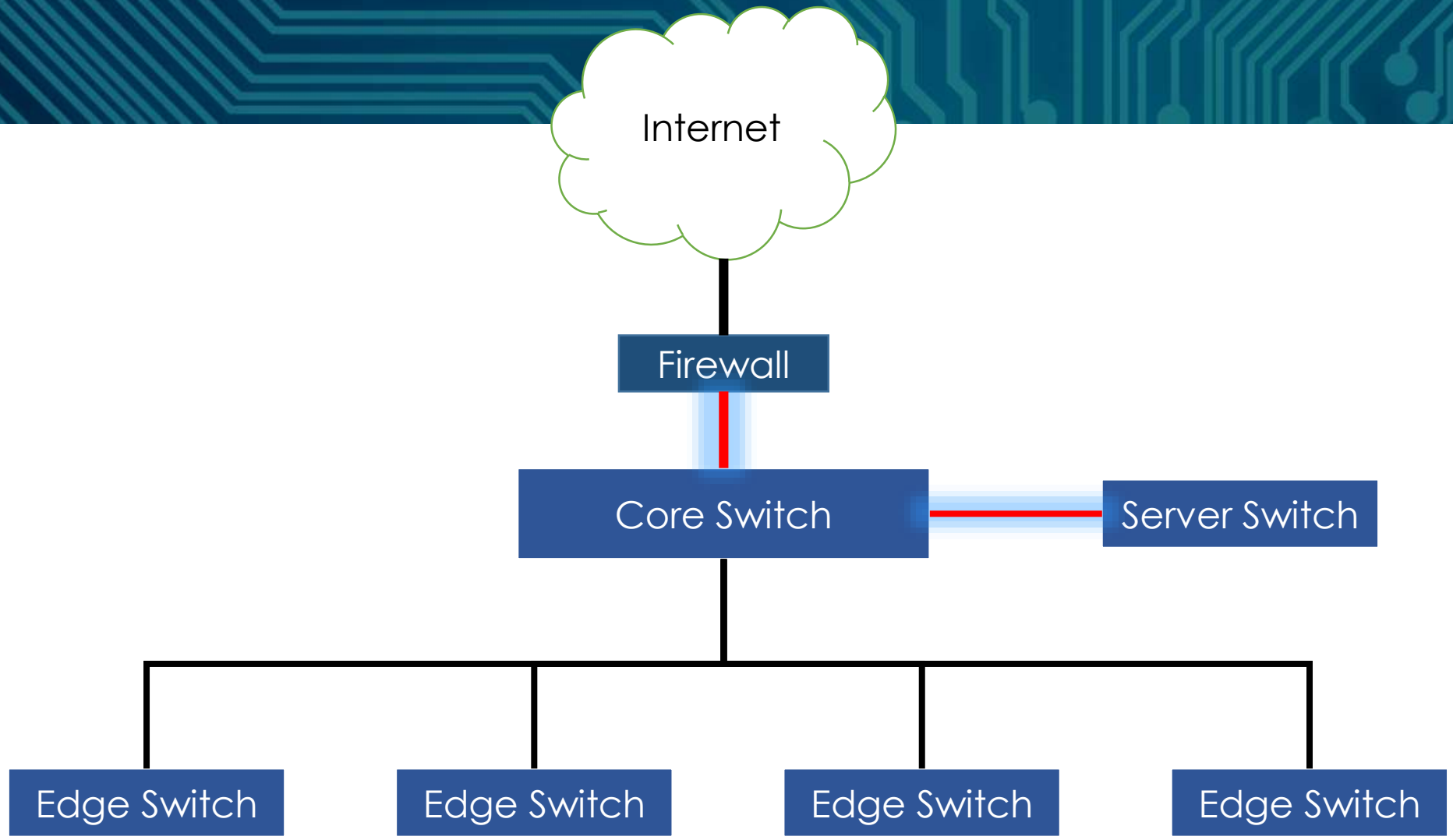
What is The Interesting Data?

- Network connection details
  - Source and Destination IP & Port
  - Protocol Information
  - Connection State
- DNS Requests
- DHCP Assignments
- HTTP Requests

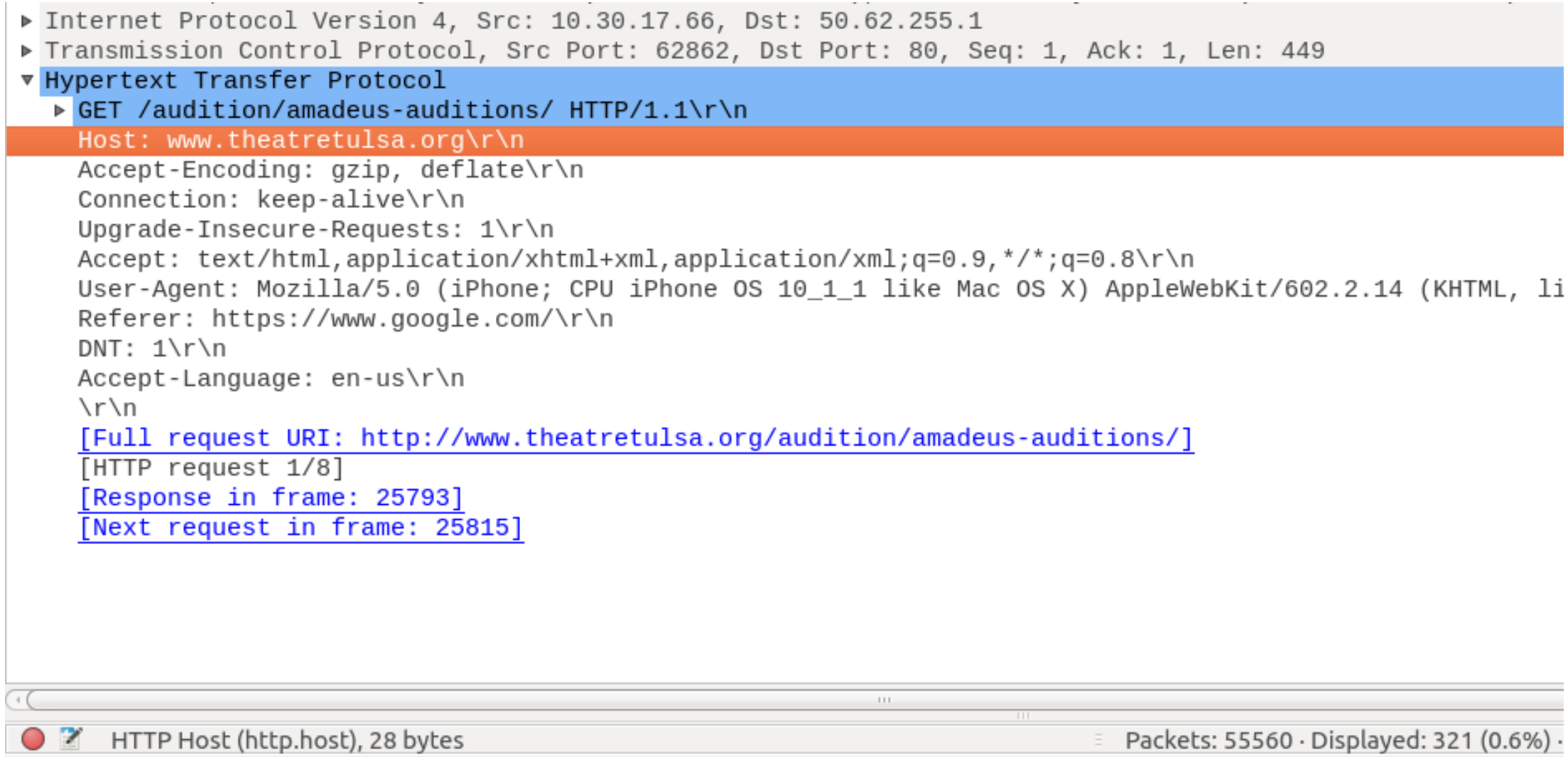

How do you collect it?

How do you collect it?

- Mirror ports or Network taps
- Placement is key
  - Insert in a place where interesting traffic will flow
    - At the network border
    - Between client and server networks
  - Change your network topology if needed
- Tap Aggregation
  - Combine several taps into one output


Internet
Firewall
Core Switch
Server Switch
Edge Switch
Edge Switch
Edge Switch
Edge Switch

Wireshark Example



How Do You Collect It?

- Bro Network Security Monitor
  - http://www.bro.org/
  - Fully passive traffic analysis off a network tap
  - Comprehensive logging of activity for forensics
  - Support for many application-layer protocols
    - DNS, FTP, HTTP, IRC, SMTP, SSH, SSL, etc…

Bro Log Example – conn.log


```
{
"ts": 1500310758.9116,
"uid": "Cuj5Ui0hNjQwxBZr2",
"id.orig_h": "10.30.17.66",
"id.orig_p": 62862,
"id.resp_h": "50.62.255.1",
"id.resp_p": 80,
"proto": "tcp",
"service": "http",
"duration": 11.649768,
"orig_bytes": 3478,
"resp_bytes": 336832,
"conn_state": "SF",
"local_orig": true,
"local_resp": false,
"missed_bytes": 203253,
"history": "ShADadtcfF",
"orig_pkts": 182,
"orig_ip_bytes": 12954,
"resp_pkts": 112,
"resp_ip_bytes": 149099,
"tunnel_parents": [  ]
}
```

Bro Log Example – http.log


```
{
"ts": 1500310758.9826,
"uid": "Cuj5Ui0hNjQwxBZr2",
"id.orig_h": "10.30.17.66",
"id.orig_p": 62862,
"id.resp_h": "50.62.255.1",
"id.resp_p": 80,
"trans_depth": 1,
"method": "GET",
"host": "www.theatretulsa.org",
"uri": "\/audition\/amadeus-auditions\/",
"user_agent": "Mozilla\/5.0 (iPhone; CPU iPhone OS 10_1_1 like Mac OS X)
AppleWebKit\/602.2.14 (KHTML, like Gecko) Version\/10.0 Mobile\/14B100
Safari\/602.1",
"referrer": "https:\/\/www.google.com\/",
"version": "1.1",
"request_body_len": 0,
"response_body_len": 42910,
"status_code": 200,
"status_msg": "OK",
"tags": [ ],
"resp_fuids": [ "Fe2BNf4EtOZGGyffYi" ],
"resp_mime_types": [ "text\/html" ]
}
```

Bro Log Example – http.log (x8)

"uri":"/audition/amadeus-auditions/"

"uri":"/wp-includes/js/wp-emoji-release.min.js?ver=4.7.5"

"uri":"/wp-content/themes/Divi/epanel/shortcodes/css/shortcodes.css?ver=3.0"

"uri":"/wp-content/themes/Divi/epanel/shortcodes/css/shortcodes_responsive.css?ver=3.0"

"uri":"/wp-includes/js/jquery/jquery.js?ver=1.12.4"

"uri":"/wp-content/themes/Divi/includes/builder/scripts/frontend-builder-scripts.js?ver=2.5.5"

"uri":"/wp-content/uploads/2015/10/93TT_Brochure-BKG-s1_rev3-TULLCa.jpg"

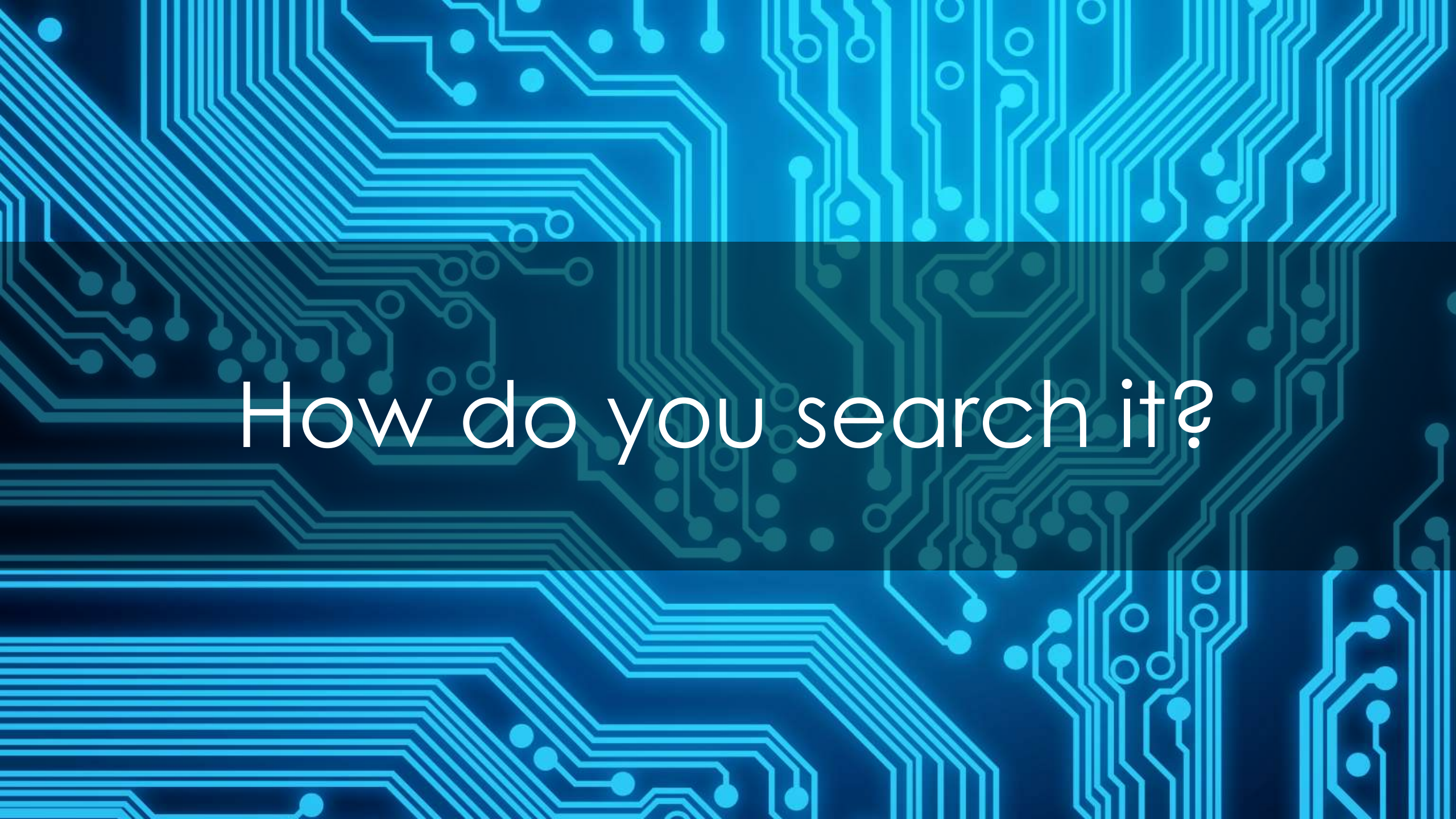
"uri":"/wp-content/plugins/jetpack/_inc/genericons/genericons/Genericons.svg"

Bro Log Example – files.log


```
{
"ts": 1500310761.4586,
"fuid": "Fe2BNf4EtOZGGyffYi",
"tx_hosts": [ "50.62.255.1" ],
"rx_hosts": [ "10.30.17.66" ],
"conn_uids": ["Cuj5Ui0hNjQwxBZr2"],
"source": "HTTP",
"depth": 0,
"analyzers": [ "MD5", "SHA1" ],
"mime_type": "text\/html",
"duration": 0.008051,
"local_orig": false,
"is_orig": false,
"seen_bytes": 42910,
"missing_bytes": 0,
"overflow_bytes": 0,
"timedout": false,
"md5": "fa7fa21df2e0e30f425e6f2fed51755c",
"sha1": "6ff743f581caceda059ac3e13e8f99c578f67df9"
}
```

Bro Logs

- conn.log
- dce_rpc.log
- dhcp.log
- dns.log
- dpd.log
- files.log
- http.log
- kerberos.log
- known_hosts.log
- known_services.log
- notice.log
- ntlm.log
- snmp.log
- software.log
- ssl.log
- stats.log
- weird.log
- x509.log


How do you search it?

How do you search it?

Log Input
+
Enrichment

Log Storage
+
Search API

Search UI

Logstash Configuration

```
input {
  file {
    path => ‘/usr/local/bro/logs/current/*.log’
  }
}
filter {
  date {
    match => [‘ts’,’UNIX’]
  }
}
output {
  elasticsearch {
  }
}
```

kibana

17,411 hits

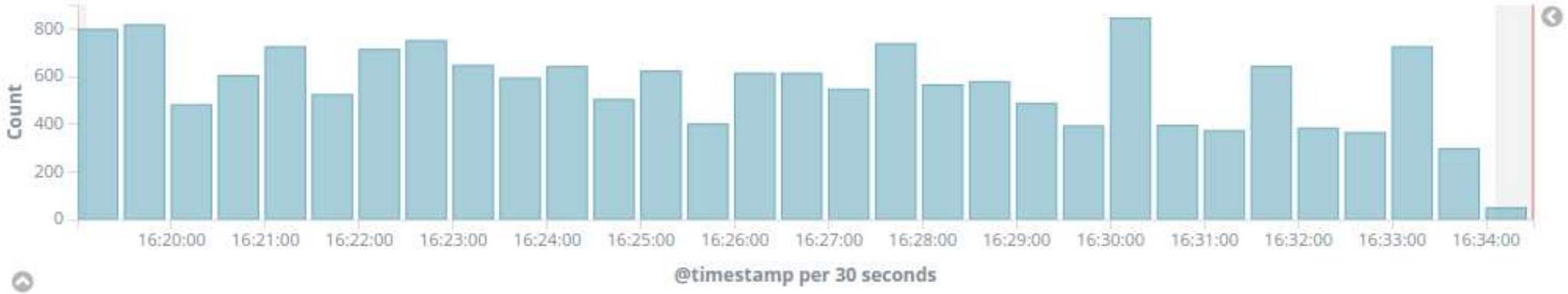
New Save Open Share Last 15 minutes

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter +

- Discover
- Visualize
- Dashboard
- Timelion
- Dev Tools
- Management

July 18th 2017, 16:19:05.826 - July 18th 2017, 16:34:05.826 — Auto



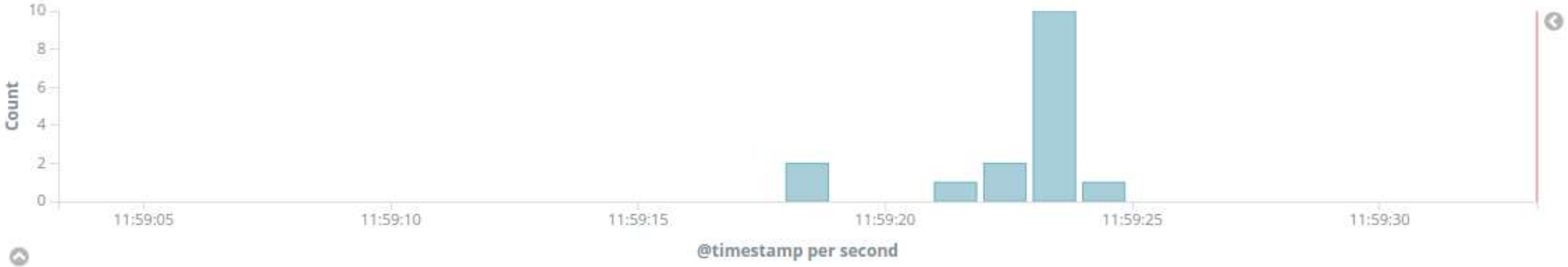
Time	_source
July 18th 2017, 16:34:03.522	id.orig_p: 62,784 id.resp_p: 5,355 tags: _geoip_lookup_failure uid: Cji4KVy3LgtBTGOpf path: /usr/local/bro/logs/current/weird.log @timestamp: July 18th 2017, 16:34:03.522 peer: bro name: dns_unmatched_msg @version: 1 host: techfest id.orig_h: fe80::11b0:a82c:d2f0:49b2 ts: 1,500,413,643.523 id.resp_h: ff02::1:3 notice: false _id: AV1Xn07NHKUevFxD2l5L _type: logs _index: logstash-2017.07.18 _score: -
July 18th 2017, 16:34:03.162	TTLs: 108, 108, 108 qclass_name: C_INTERNET qtype_name: A qtype: 1 rejected: false id.resp_p: 53 answers: 216.155.194.12, 74.6.34.29, 74.6.105.13 trans_id: 55,182 uid: C818aU37sNAH9X0w57 path: /usr/local/bro/logs/current/dns.log @version: 1 host: techfest id.orig_h: 10.30.19.24 Z: 0 qclass: 1 id.resp_h: 129.244.3.254 geo-dest.timezone: America/Chicago geo-dest.ip: 129.244.3.254 geo-dest.latitude: 36.147 geo-dest.continent_code: NA geo-dest.city_name: Tulsa geo-
July 18th 2017, 16:34:03.162	TTLs: 4,618, 7 qclass_name: C_INTERNET qtype_name: A qtype: 1 rejected: false id.resp_p: 53

Collapse

CuJ5Ui0hNjQwxBZr2 Uses lucene query syntax

Add a filter +

July 17th 2017, 11:59:03.273 - July 17th 2017, 11:59:33.189 — Auto



Time	_source
July 17th 2017, 11:59:24.190	uid: Cuj5Ui0hNjQwxBZr2 id.orig_p: 62,862 method: GET request_body_len: 0 id.resp_p: 80 uri: /wp-content/plugins/jetpack/_inc/genericons/genericons/Genericons.svg tags: _geoip_lookup_failure referrer: http://www.theatretulsa.org/audition/amadeus-auditions/ path: /usr/local/bro/logs/current/http.log trans_depth: 8 @timestamp: July 17th 2017, 11:59:24.190 host: www.theatretulsa.org @version: 1 id.orig_h: 10.30.17.66 response_body_len: 0 user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 10_1_1 like Mac OS X) AppleWebKit/602.2.14 (KHTML, like Gecko) Version/10.0 Mobile/14B100 Safari/
July 17th 2017, 11:59:23.822	conn_uids: Cuj5Ui0hNjQwxBZr2 timedout: true local_orig: false rx_hosts: 10.30.17.66 source: HTTP is_orig: false tx_hosts: 50.62.255.1 overflow_bytes: 0 tags: _geoip_lookup_failure duration: 0.592 path: /usr/local/bro/logs/current/files.log depth: 0 @timestamp: July 17th 2017, 11:59:23.822 analyzers: MD5, SHA1 @version: 1 host: techfest fuid: FAJGdn2st5FB6OaFa3 seen_bytes: 0 missing_bytes: 191,247 ts: 1,500,310,763.823 _id: AV1RgScyHKUevFxDk9rF _type: logs _index: logstash-2017.07.17 _score: -
July 17th 2017, 11:59:23.742	uid: Cuj5Ui0hNjQwxBZr2 id.orig_p: 62,862 method: GET request_body_len: 0 id.resp_p: 80 uri: /wp-content/uploads/2

@timestamp	July 17th 2017, 11:59:18.911
@version	1
_id	AV1RfaviHKUevFxDk7Jk
_index	logstash-2017.07.17
_score	-
_type	logs
conn_state	SF
duration	11.65
geo-dest.city_name	Scottsdale
geo-dest.continent_code	NA
geo-dest.country_code2	US
geo-dest.country_code3	US
geo-dest.country_name	United States
geo-dest.dma_code	753
geo-dest.ip	50.62.255.1
geo-dest.latitude	33.612
geo-dest.location.lat	33.612
geo-dest.location.lon	-111.891
geo-dest.longitude	-111.891
geo-dest.postal_code	85260
geo-dest.region_code	AZ
geo-dest.region_name	Arizona
geo-dest.timezone	America/Phoenix
history	ShADadtcfF
host	techfest

CuJ5Ui0hNjQwxBZr2 Uses lucene query syntax

path.keyword: "/usr/local/bro/logs/current/http.log" Add a filter + Actions

July 17th 2017, 11:59:03.273 - July 17th 2017, 11:59:33.189 — Auto

Time	uri
July 17th 2017, 11:59:24.190	/wp-content/plugins/jetpack/_inc/genericons/genericons/Genericons.svg
July 17th 2017, 11:59:23.742	/wp-content/uploads/2015/10/93TT_Brochure-BKG-s1_rev3-TULLCa.jpg
July 17th 2017, 11:59:23.490	/wp-content/themes/Divi/includes/builder/scripts/frontend-builder-scripts.js?ver=2.5.5
July 17th 2017, 11:59:23.246	/wp-includes/js/jquery/jquery.js?ver=1.12.4
July 17th 2017, 11:59:23.158	/wp-content/themes/Divi/epanel/shortcodes/css/shortcodes_responsive.css?ver=3.0
July 17th 2017, 11:59:23.058	/wp-content/themes/Divi/epanel/shortcodes/css/shortcodes.css?ver=3.0
July 17th 2017, 11:59:22.886	/wp-includes/js/wp-emoji-release.min.js?ver=4.7.5
July 17th 2017, 11:59:18.982	/audition/amadeus-auditions/

55 hits

New Save Open Share July 17th 2017, 11:59:03.273 to July 17th 2017, 11:59:33.189

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

path.keyword: "/usr/local/bro/logs/current/http.log" id.orig_h: "10.30.17.66" Add a filter + Actions

July 17th 2017, 11:59:03.273 - July 17th 2017, 11:59:33.189 — Auto

Time	host	uri
July 17th 2017, 11:59:24.534	graph.facebook.com	/?callback=WPCOMSharing.update_facebook_count&ids=http://www.theatretulsa.org/audition/amadeus-auditions/&_=1500310900300
July 17th 2017, 11:59:24.534	pixel.wp.com	/g.gif?v=wpcom-no-pv&x_sharing-count-request=facebook&r=0.41387511667957655
July 17th 2017, 11:59:24.502	api.pinterest.com	/v1/urls/count.json?callback=WPCOMSharing.update_pinterest_count&url=http://www.theatretulsa.org/audition/amadeus-auditions/&_=1500310900299
July 17th 2017, 11:59:24.502	pixel.wp.com	/g.gif?v=wpcom-no-pv&x_sharing-count-request=twitter&r=0.45042016569265464
July 17th 2017, 11:59:24.502	pixel.wp.com	/g.gif?v=wpcom-no-pv&x_sharing-count-request=pinterest&r=0.8851506339894292
July 17th 2017, 11:59:24.414	s.gravatar.com	/css/services.css?ver=2017Julaa
July 17th 2017, 11:59:24.390	s.gravatar.com	/css/hovercard.css?ver=2017Julaa

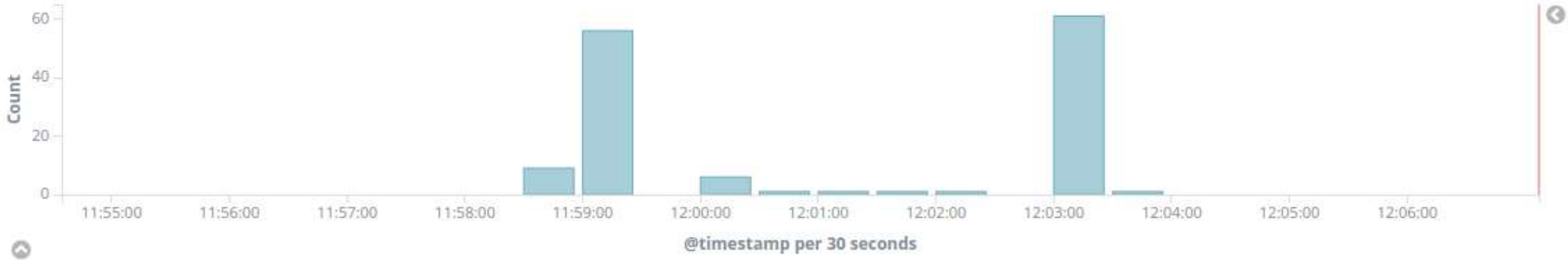
137 hits

New Save Open Share July 17th 2017, 11:54:34.576 to July 17th 2017, 12:07:07.118

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

path.keyword: "/usr/local/bro/logs/current/http.log" id.orig_h: "10.30.17.66" Add a filter + Actions

July 17th 2017, 11:54:34.576 - July 17th 2017, 12:07:07.118 — Auto



Time	host	uri
July 17th 2017, 12:03:30.022	gsp1.apple.com	/pep/gcc
July 17th 2017, 12:03:27.178	gsp1.apple.com	/pep/gcc
July 17th 2017, 12:03:26.710	gsp1.apple.com	/pep/gcc
July 17th 2017, 12:03:25.410	gsp1.apple.com	/pep/gcc
July 17th 2017, 12:03:23.938	gsp1.apple.com	/pep/gcc
July 17th 2017, 12:03:11.206	api.pin	/v1/urls/count.json?

Basic Charts


Area


Heat Map


Horizontal Bar


Line


Pie


Vertical Bar

Data


Data Table


Gauge

Goal

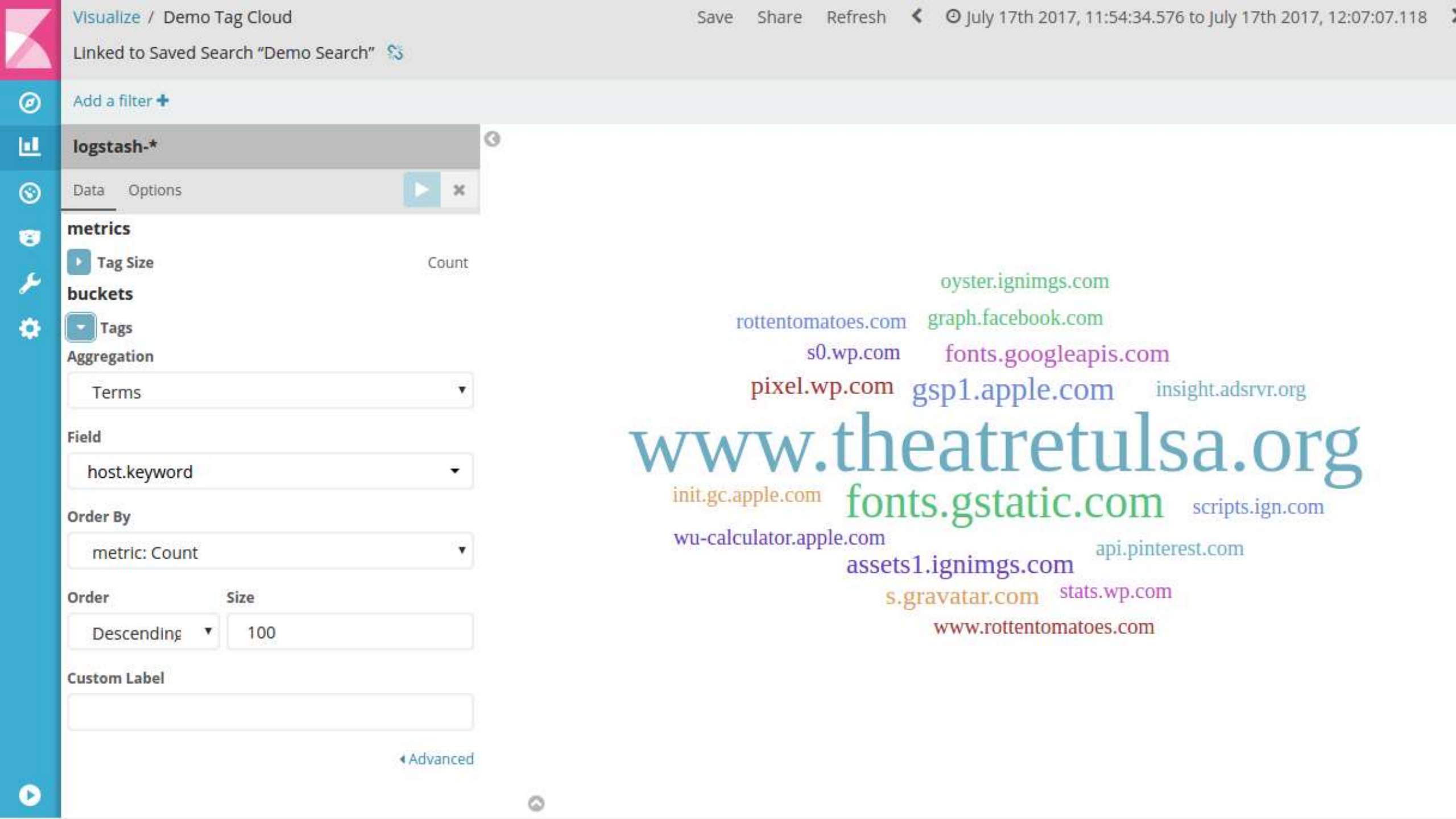
Metric

Maps


Coordinate Map


Region Map

Time Series


Visualize / Demo Tag Cloud
Save
Share
Refresh
July 17th 2017, 11:54:34.576 to July 17th 2017, 12:07:07.118
Linked to Saved Search "Demo Search"
Add a filter +
logstash-*
Data
Options
metrics
Tag Size
Count
buckets
Tags
Aggregation
Terms
Field
host.keyword
Order By
metric: Count
Order
Descending
Size
100
Custom Label
Advanced
oyster.ignimgs.com
rottentomatoes.com
graph.facebook.com
s0.wp.com
fonts.googleapis.com
pixel.wp.com
gsp1.apple.com
insight.adsrvr.org
www.theatretulsa.org
init.gc.apple.com
fonts.gstatic.com
scripts.ign.com
wu-calculator.apple.com
api.pinterest.com
assets1.ignimgs.com
s.gravatar.com
stats.wp.com
www.rottentomatoes.com

logstash-*

Data | Metrics & Axes | Panel Settings

metrics

Y-Axis Count

Add metrics

buckets

X-Axis

Aggregation: Terms

Field: geo-dest.region_name.keyword

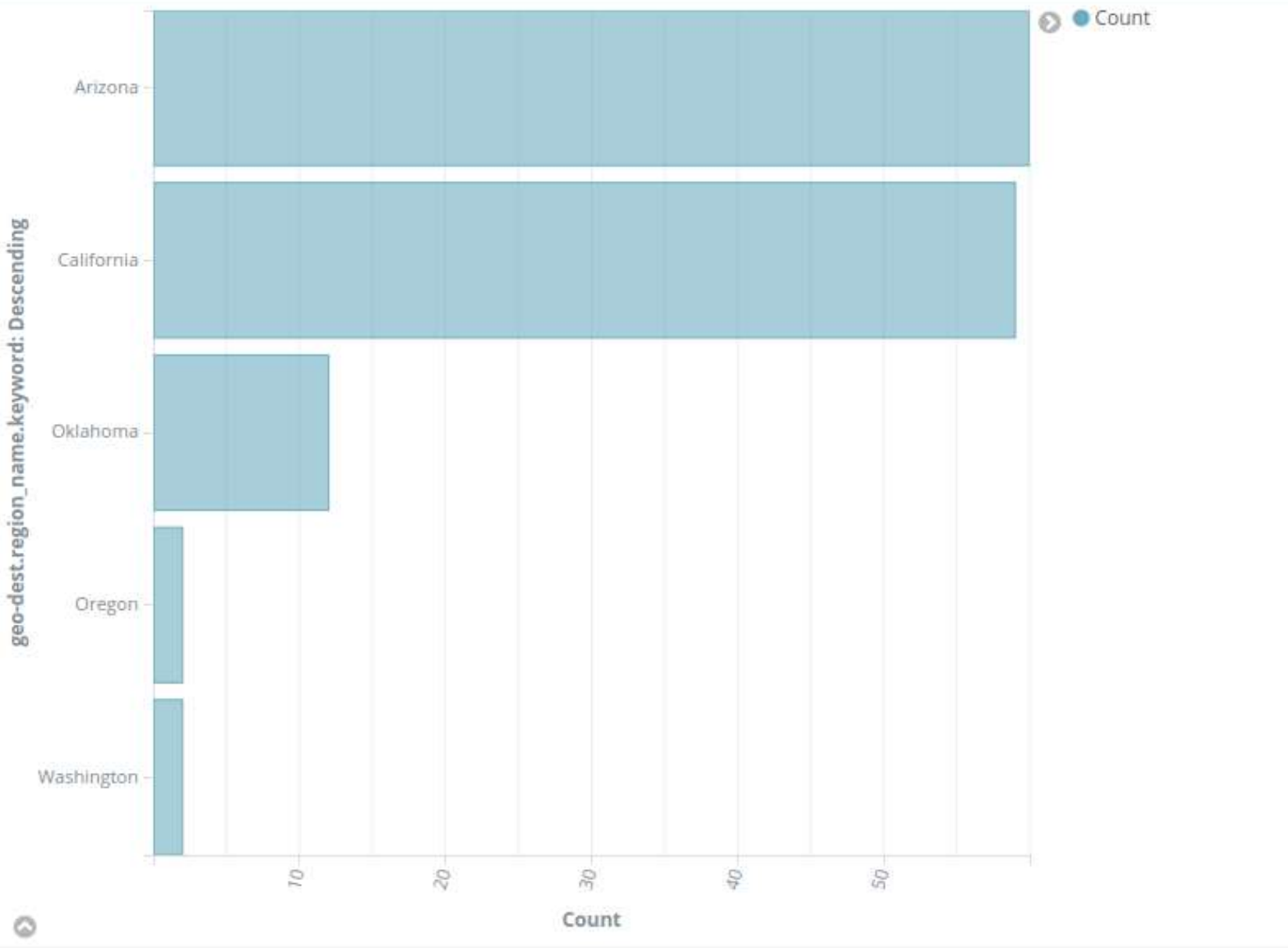
Order By: metric: Count

Order: Descendin | Size: 5

Custom Label:

Advanced

Add sub-buckets



Add a filter +

logstash-*

Data | Metrics & Axes | Panel Settings

metrics

Y-Axis

Aggregation

Unique Count

Field

geo-dest.region_name.keyword

Custom Label

Advanced

Add metrics

buckets

X-Axis

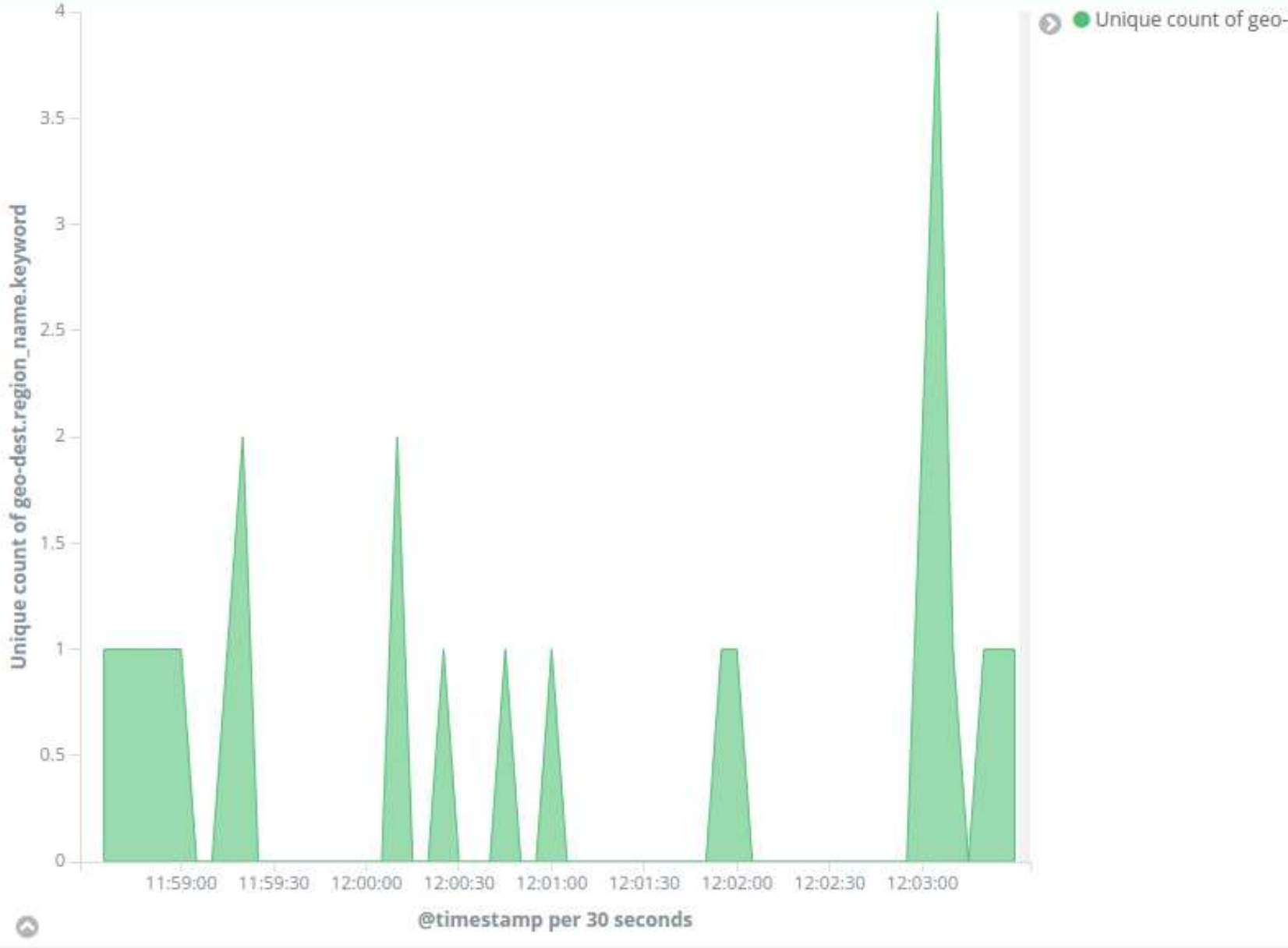
Aggregation

Date Histogram

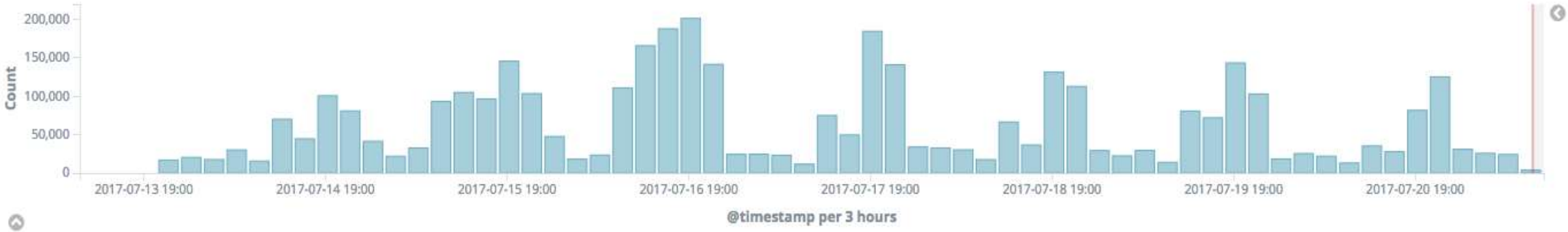
Field

@timestamp

Interval



July 13th 2017, 10:31:50.184 - July 21st 2017, 10:31:50.184 — Auto



Time	_source
July 21st 2017, 10:31:31.904	conn_state: SF resp_pkts: 8 id.resp_p: 443 duration: 0.34 local_resp: false uid: CNGC0s4yxasBM0kr2b path: /usr/local/bro/logs/current/conn.log @version: 1 host: techfest id.orig_h: 10.30.19.137 id.resp_h: 34.194.208.121 geo-dest.timezone: America/New_York geo-dest.ip: 34.194.208.121 geo-dest.latitude: 39.048 geo-dest.continent_code: NA geo-dest.city_name: Ashburn geo-dest.country_name: United States geo-dest.country_code2: US geo-dest.dma_code: 511 geo-dest.country_code3: US geo-dest.region_name: Virginia geo-dest.location.lon: -77.473 geo-dest.location.lat: 39.048 geo-dest.postal_code: 20149 geo-dest.region_code: VA geo-dest.longitude: -77.473 id.orig_p: 63,861 resp_ip_bytes: 1,047 orig_bytes: 1,201 local_orig: t
July 21st 2017, 10:31:31.330	conn_state: SF resp_pkts: 15 id.resp_p: 443 duration: 0.647 local_resp: false uid: Cgjvxu1RyCGu5BSrab path: /usr/local/bro/logs/current/conn.log @version: 1 host: techfest id.orig_h: 10.30.18.201 id.resp_h: 17.134.127.79 geo-dest.timezone: America/Los_Angeles geo-dest.ip: 17.134.127.79 geo-dest.latitude: 37.304 geo-dest.continent_code: NA geo-dest.city_name: Cupertino geo-dest.country_name: United States geo-dest.country_code2: US geo-dest.dma_code: 807 geo-dest.country_code3: US geo-dest.region_name: California geo-dest.location.lon: -122.095 geo-dest.location.lat: 37.304 geo-dest.postal_code: 95014 geo-dest.region_code: CA geo-dest.longitude: -122.095 id.orig_p: 53,599 resp_ip_bytes: 5,440 orig_bytes: 995 local_orig: tr
July 21st 2017, 10:31:22.606	conn_state: SF resp_pkts: 65 id.resp_p: 80 duration: 0.198 local_resp: false uid: C0lAupZzvqRexOrWQ3 path: /usr/local/bro/logs/current/conn.log @version: 1 host: techfest id.orig_h: 10.30.19.125 id.resp_h: 208.85.44.23 geo-dest.timezone: America/Los_Angeles geo-dest.ip: 208.85.44.23 geo-dest.latitude: 37.804 geo-dest.continent_code: NA geo-dest.city_name: Oakland geo-dest.country_name: United States geo-dest.country_code2: US geo-dest.dma_code: 807 geo-dest.country_code3: US geo-dest.region_name: California geo-dest.location.lon: -122.271 geo-dest.location.lat: 37.804 geo-

Add a filter +

logstash-*

Data | Metrics & Axes | Panel Settings

metrics

Y-Axis

Aggregation: Unique Count

Field: id.orig_h.keyword

Custom Label: Unique Hosts

Advanced

Add metrics

buckets

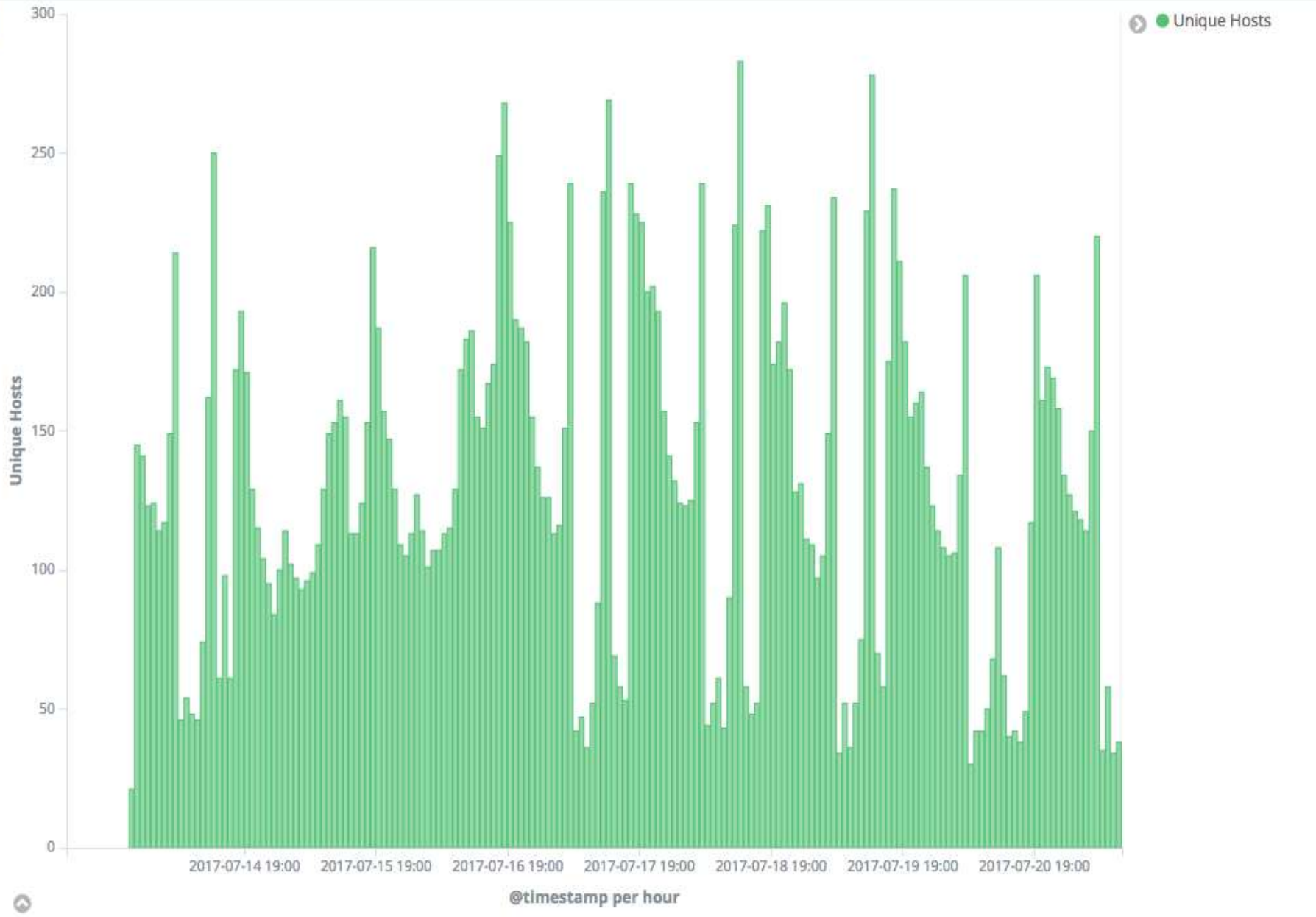
X-Axis

Aggregation: Date Histogram

Field: @timestamp

Interval: Hourly

Custom Label



logstash-*

Data Options

metrics

Tag Size Count

buckets

Tags

Aggregation

Terms

Field

geo-dest.country_name.keyword

Order By

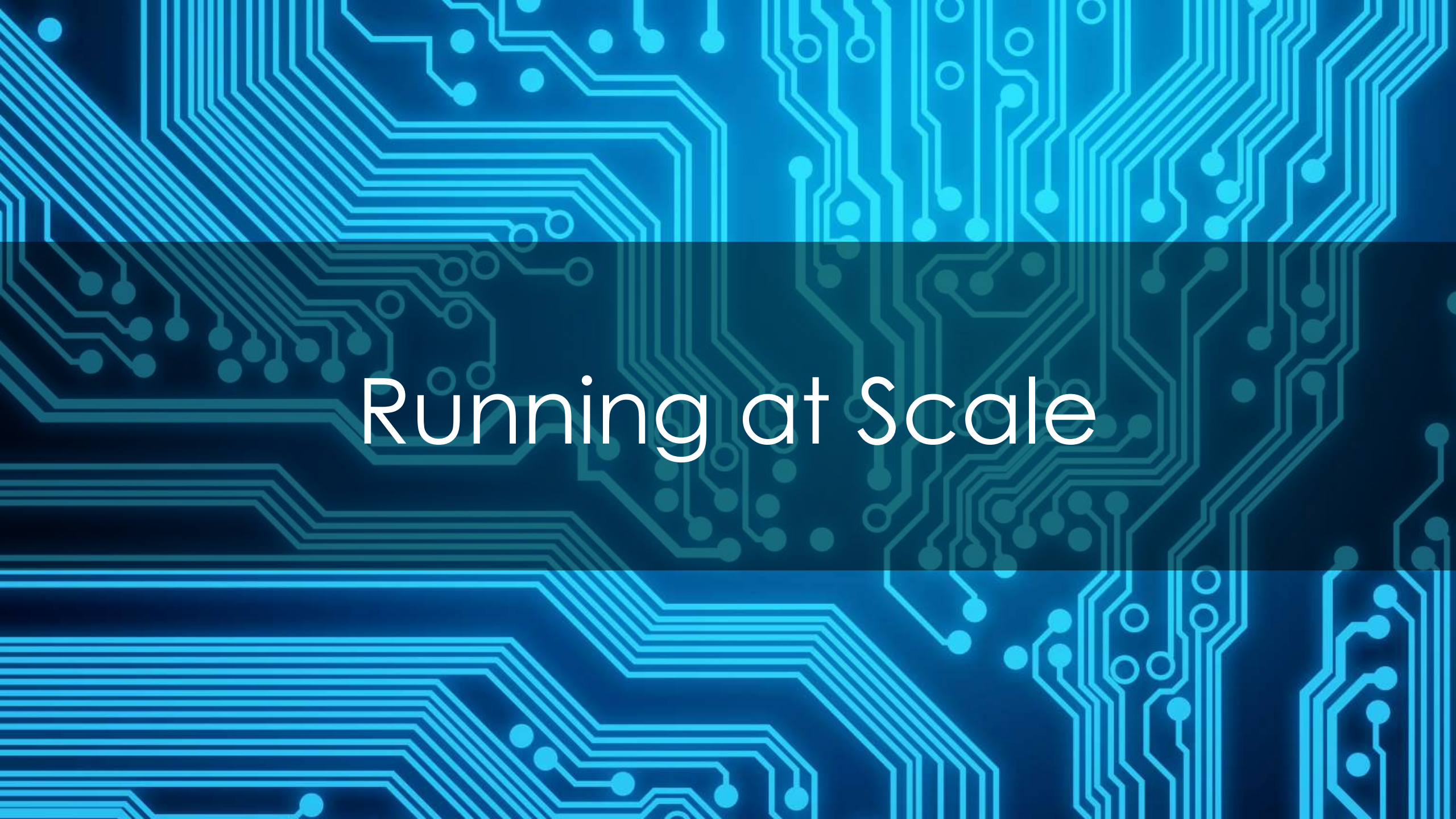
metric: Count

Order Size

Descending 50

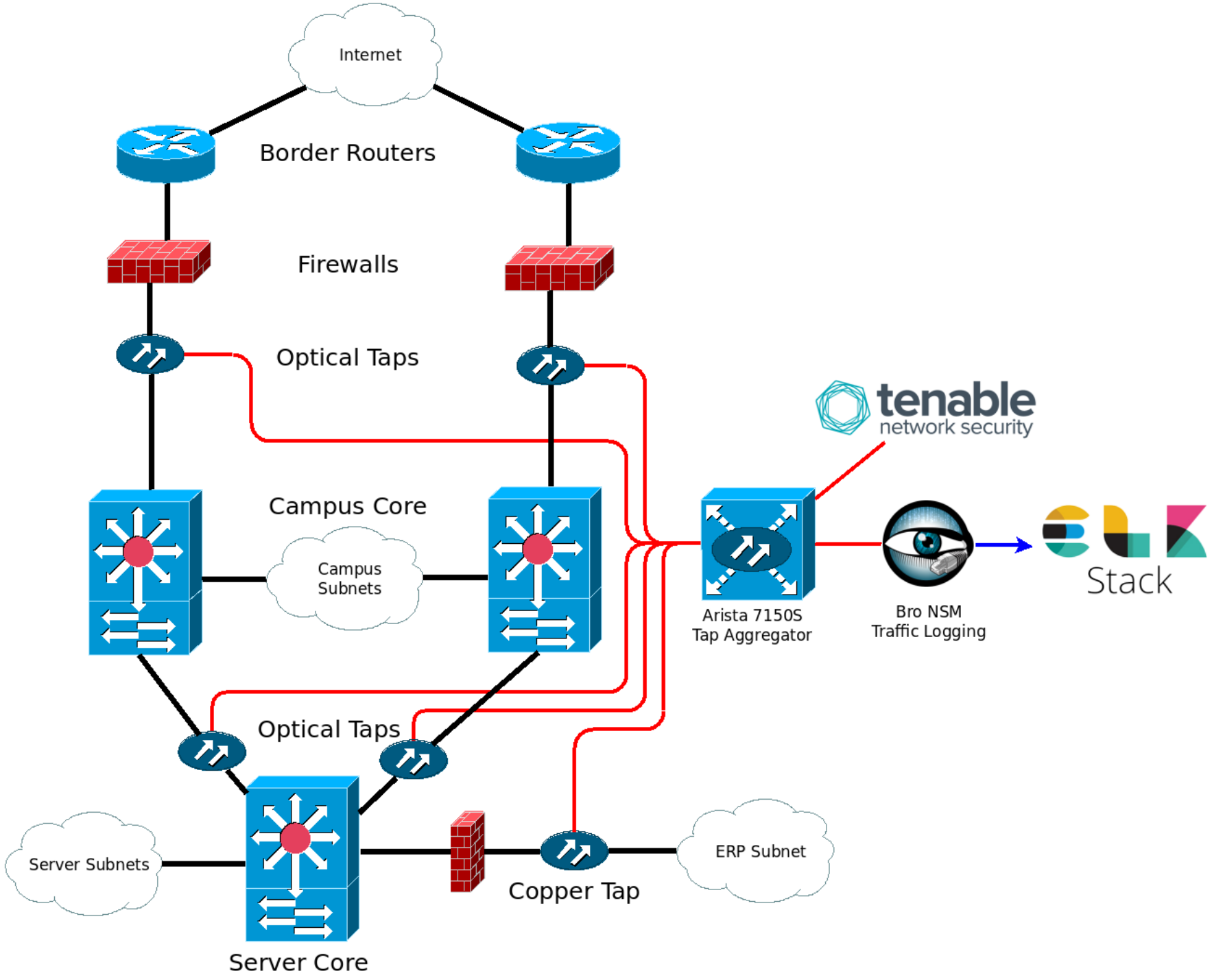
Custom Label

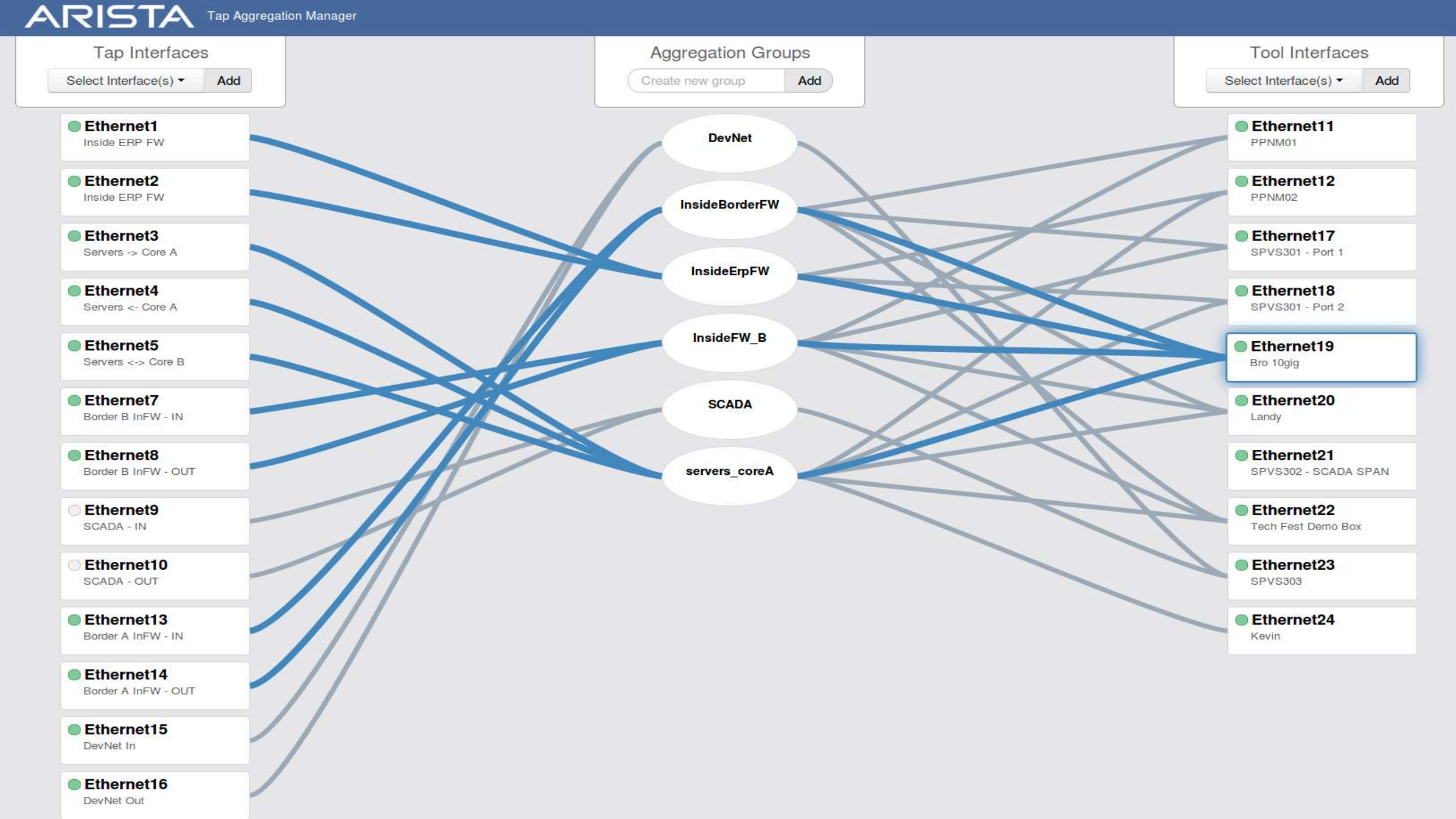
Advanced


Running at Scale

Running at Scale

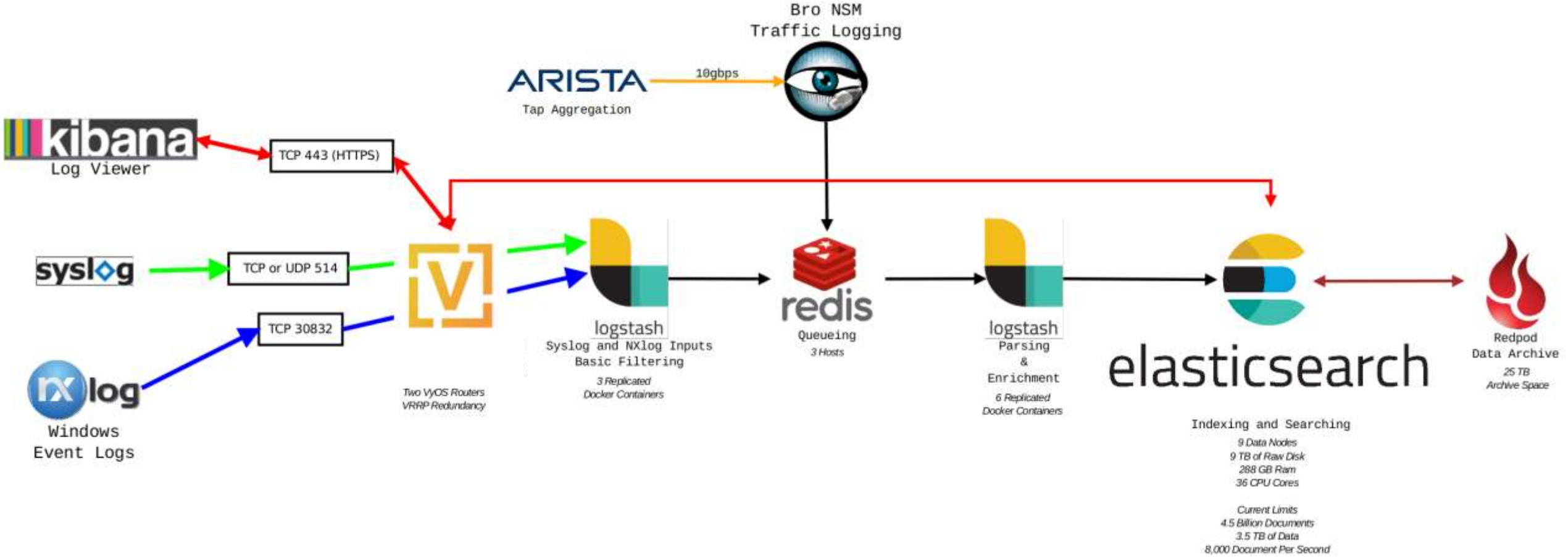
- 6 tap points
  - 3 optical 10gig taps
  - 2 copper 1gig tap
  - 1 optical 10gig mirror port
  - 11 tap inputs to aggregator
- 1 Bro Server
  - 10gig input
  - Custom compiled capture driver – PF_ring clustered mode
- 3 Redis nodes
  - Log buffering
  - Not clustered, planning to replace with Kafka cluster


Internet
Border Routers
Firewalls
Optical Taps
Campus Core
Campus
Subnets
Optical Taps
Server Subnets
Server Core
Copper Tap
ERP Subnet
tenable
network security
Arista 7150S
Tap Aggregator
Bro NSM
Traffic Logging
Stack

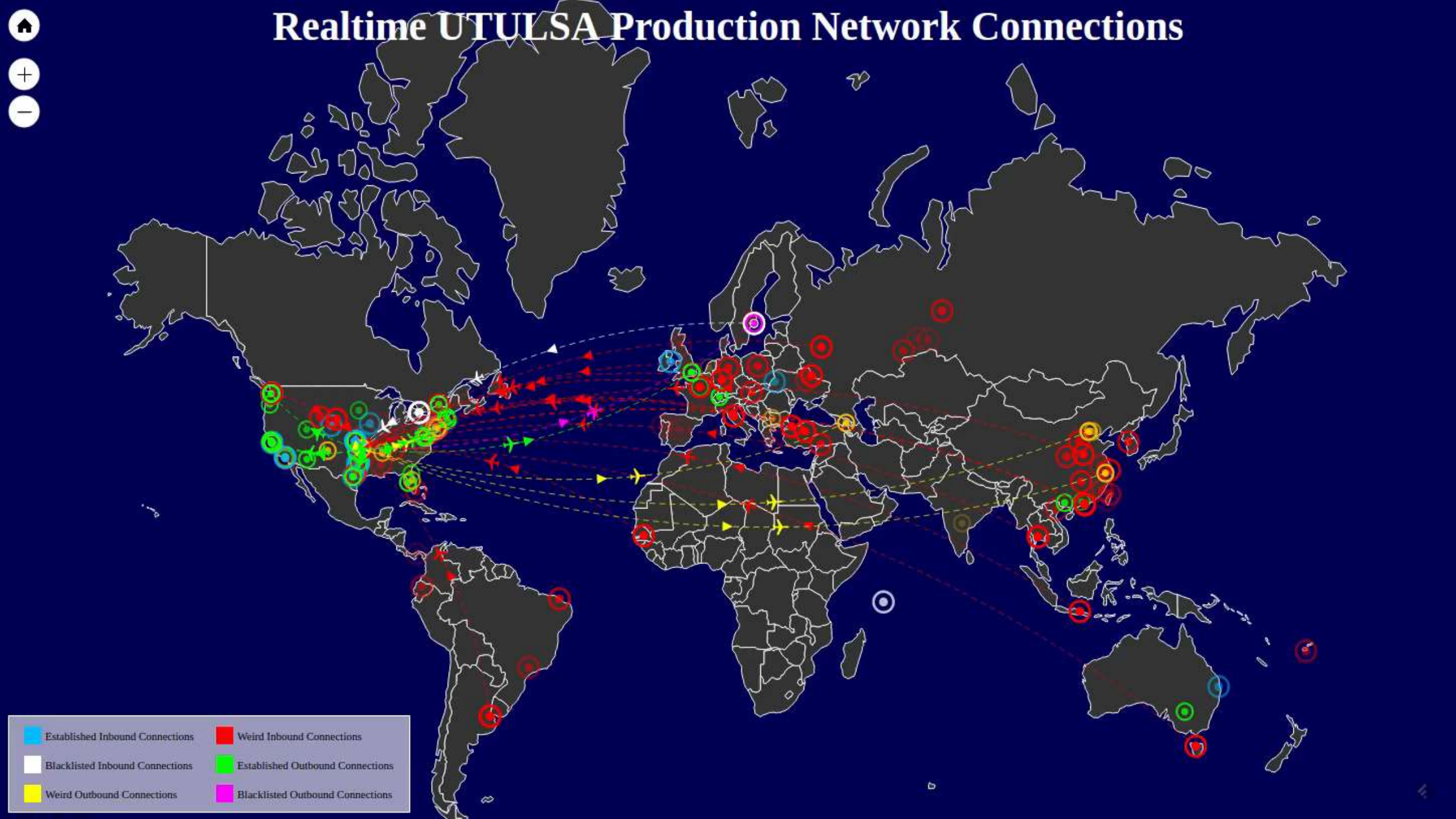

ARISTA
Tap Aggregation Manager
Tap Interfaces
Select Interface(s)
Add
Aggregation Groups
Create new group
Add
Tool Interfaces
Select Interface(s)
Add
Ethernet1
Inside ERP FW
Ethernet2
Inside ERP FW
Ethernet3
Servers -> Core A
Ethernet4
Servers <- Core A
Ethernet5
Servers <-> Core B
Ethernet7
Border B InFW - IN
Ethernet8
Border B InFW - OUT
Ethernet9
SCADA - IN
Ethernet10
SCADA - OUT
Ethernet13
Border A InFW - IN
Ethernet14
Border A InFW - OUT
Ethernet15
DevNet In
Ethernet16
DevNet Out
DevNet
InsideBorderFW
InsideErpFW
InsideFW_B
SCADA
servers_coreA
Ethernet11
PPNM01
Ethernet12
PPNM02
Ethernet17
SPVS301 - Port 1
Ethernet18
SPVS301 - Port 2
Ethernet19
Bro 10gig
Ethernet20
Landy
Ethernet21
SPVS302 - SCADA SPAN
Ethernet22
Tech Fest Demo Box
Ethernet23
SPVS303
Ethernet24
Kevin

Running at Scale

- 9 Logstash Containers
  - 3 Syslog / windows input
  - 6 Indexers
- 12 Elasticsearch Nodes
  - 3 Masters
  - 9 Data Nodes
    - Quad core, 32 GB RAM, 1 TB disk
- 1 Archive Server
  - 25 TB for snapshot archival
- Several misc. servers / containers
  - Automation, scripts, other data processors

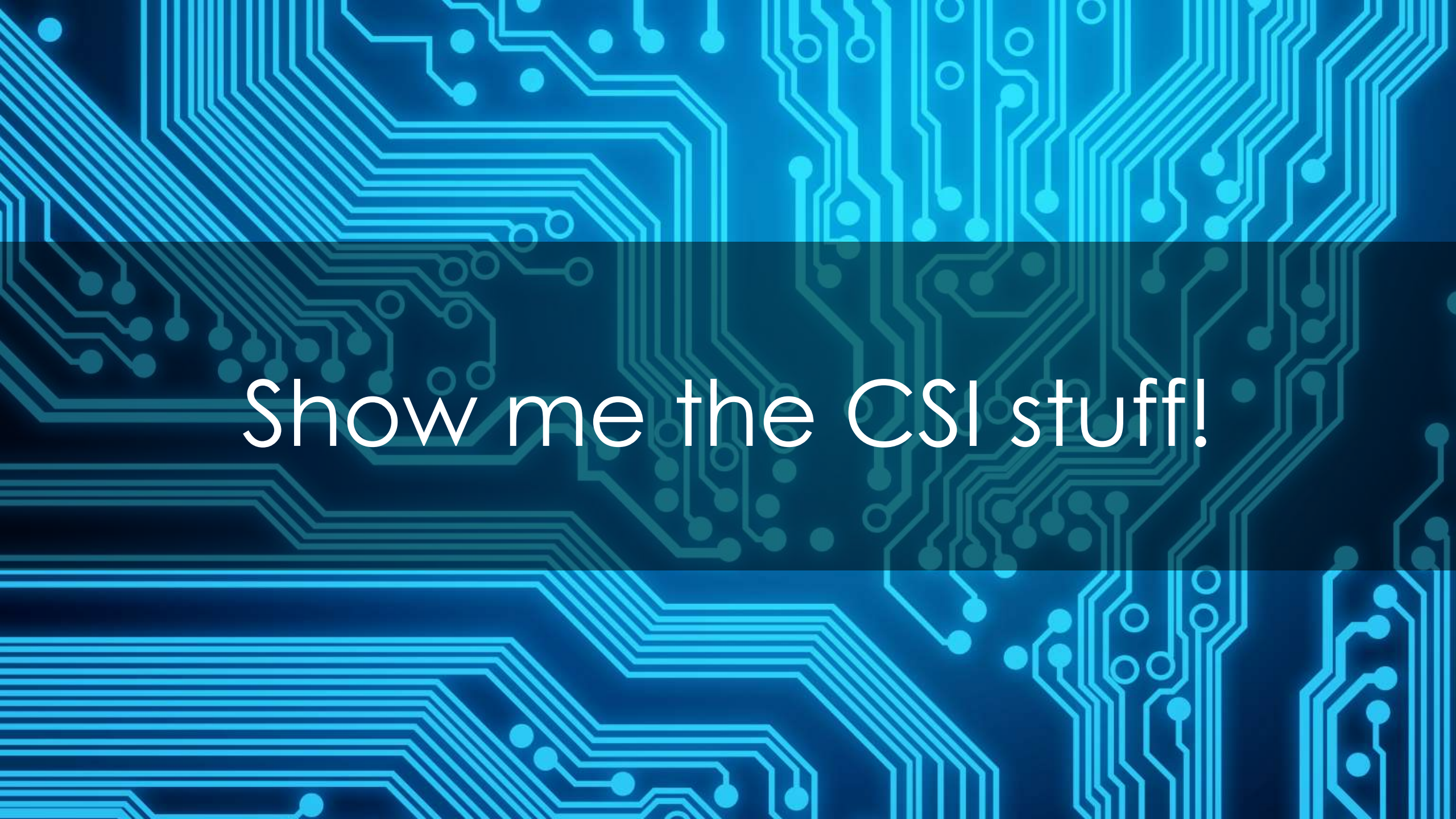

Bro NSM
Traffic Logging
ARISTA
10gbps
Tap Aggregation
kibana
Log Viewer
TCP 443 (HTTPS)
syslog
TCP or UDP 514
TCP 30832
nxlog
Windows
Event Logs
Two VyOS Routers
VRRP Redundancy
logstash
Syslog and NXlog Inputs
Basic Filtering
3 Replicated
Docker Containers
redis
Queueing
3 Hosts
logstash
Parsing
&
Enrichment
6 Replicated
Docker Containers
elasticsearch
Indexing and Searching
9 Data Nodes
9 TB of Raw Disk
288 GB Ram
36 CPU Cores
Current Limits
4.5 Billion Documents
3.5 TB of Data
8,000 Document Per Second
Redpod
Data Archive
25 TB
Archive Space

Realtime UTULSA Production Network Connections



Running at Scale

- Configuration Management
  - Cobbler / SaltStack
- Monitoring
  - Telegraf / InfluxDB / Grafana / PRTG
- High Availability
  - Elasticsearch Replicas
  - Docker Swarm
  - Service Discovery


Show me the CSI stuff!

Show me the CSI stuff!

- EventType[Authentication] MAC[64:A5:C3:xx:yy:zz] AP[USS-1838-D24] SSID[TUwpa] BSSID[20:B3:99:xx:yy:zz]
- EventType[Registration] MAC[28:5A:EB:xx:yy:zz] IP[0.0.0.0] AP[USS-1918-D8] SSID[TUwpa] BSSID[20:B3:99:xx:yy:zz]
- EventType[Roam] MAC[2C:0E:3D:xx:yy:zz] AP[FS-Lobby-A17] FromAP[FS-200-A10] BSSID[20:B3:99:xx:yy:zz]
- EventType[De-registration] MAC[EC:9B:F3:xx:yy:zz] BSSID[20:B3:99:xx:yy:zz]
- EventType[Authentication] MAC[A8:88:08:xx:yy:zz] AP[NVG-824-A12] SSID[TUwpa] BSSID[20:B3:99:xx:yy:zz]

Show me the CSI stuff!

- EventType[Authentication] **MAC[64:A5:C3:xx:yy:zz]** **AP[USS-1838-D24]** SSID[TUwpa] BSSID[20:B3:99:xx:yy:zz]
- EventType[Registration] **MAC[28:5A:EB:xx:yy:zz]** IP[0.0.0.0] **AP[USS-1918-D8]** SSID[TUwpa] BSSID[20:B3:99:xx:yy:zz]
- EventType[Roam] **MAC[2C:0E:3D:xx:yy:zz]** **AP[FS-Lobby-A17]** FromAP[FS-200-A10] BSSID[20:B3:99:xx:yy:zz]
- EventType[De-registration] MAC[EC:9B:F3:xx:yy:zz] BSSID[20:B3:99:xx:yy:zz]
- EventType[Authentication] **MAC[A8:88:08:xx:yy:zz]** **AP[NVG-824-A12]** SSID[TUwpa] BSSID[20:B3:99:xx:yy:zz]


Questions?
Twitter / Github: @ljb2of3

TECHFest TULSA - 2017 FRI, JUL 21ST

Complete An Evaluation Form & Win

Your input is important!

You can access Evaluation Forms at:

http://TulsaTechFest.com

$50 Best Buy Gift Card!!

Winner drawn – Midnight, Sun Jul 23rd!

Premier Sponsors

amazon web services

WORK READY OKLAHOMA

Gold Sponsors

mozilla

GABLE GOTWALS COUNSEL

NUTANIX

ROAD MAP TECHNOLOGIES

J.B. HUNT