Family Recipes

Ritchie's Last Supper

Created by Crazies

Network À La King

7 months of development

26 “volunteers”

38 page blueprint

<REDACTED> late nights

~$180,000 (not including vols)

~10,000+ hours

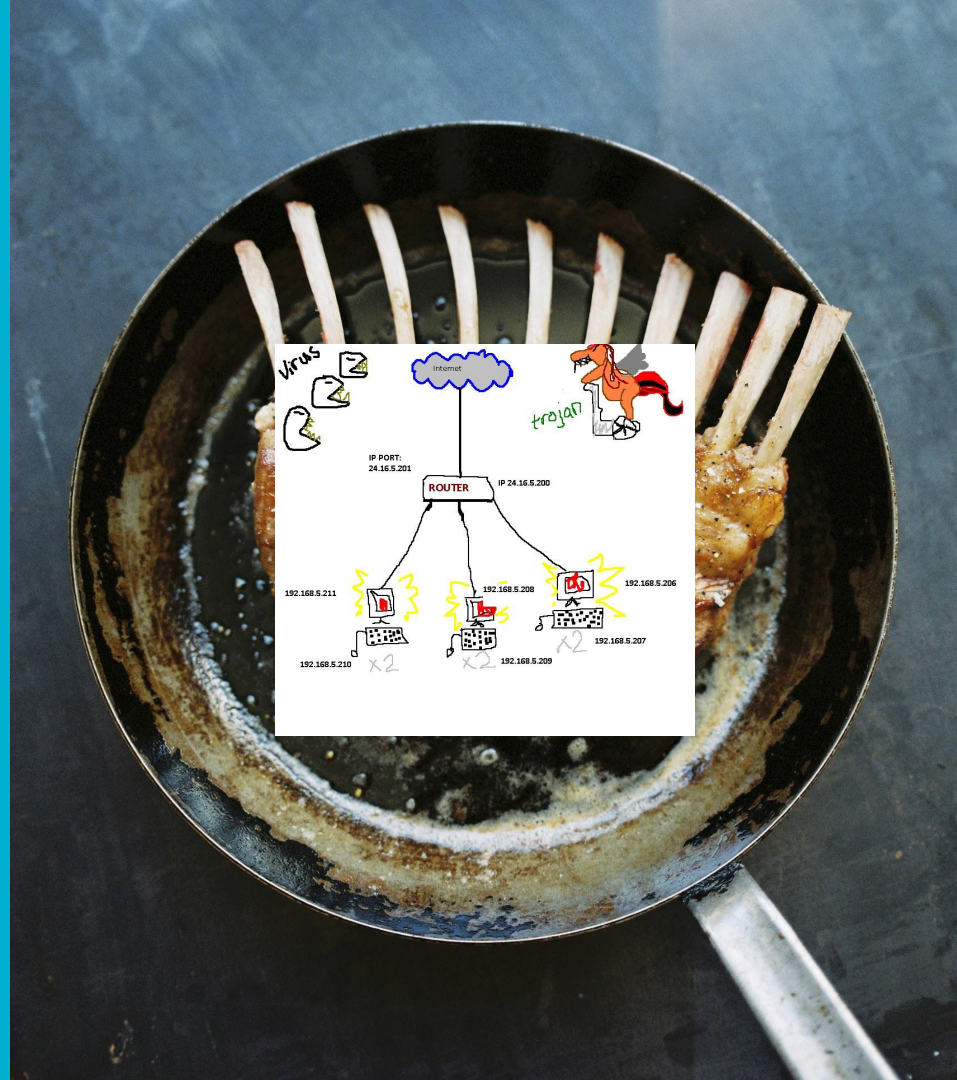
15 full online personas

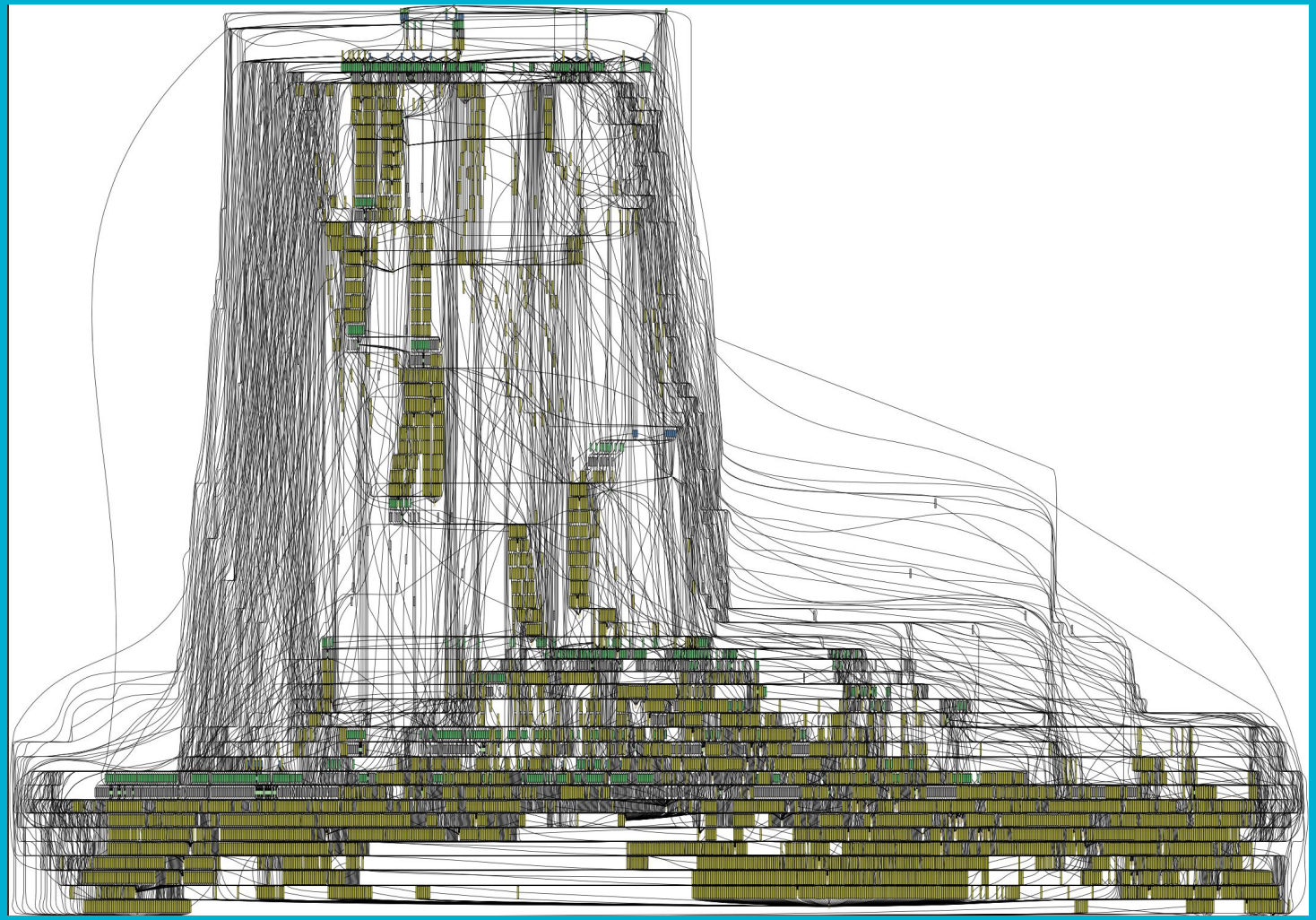
67 social media profiles

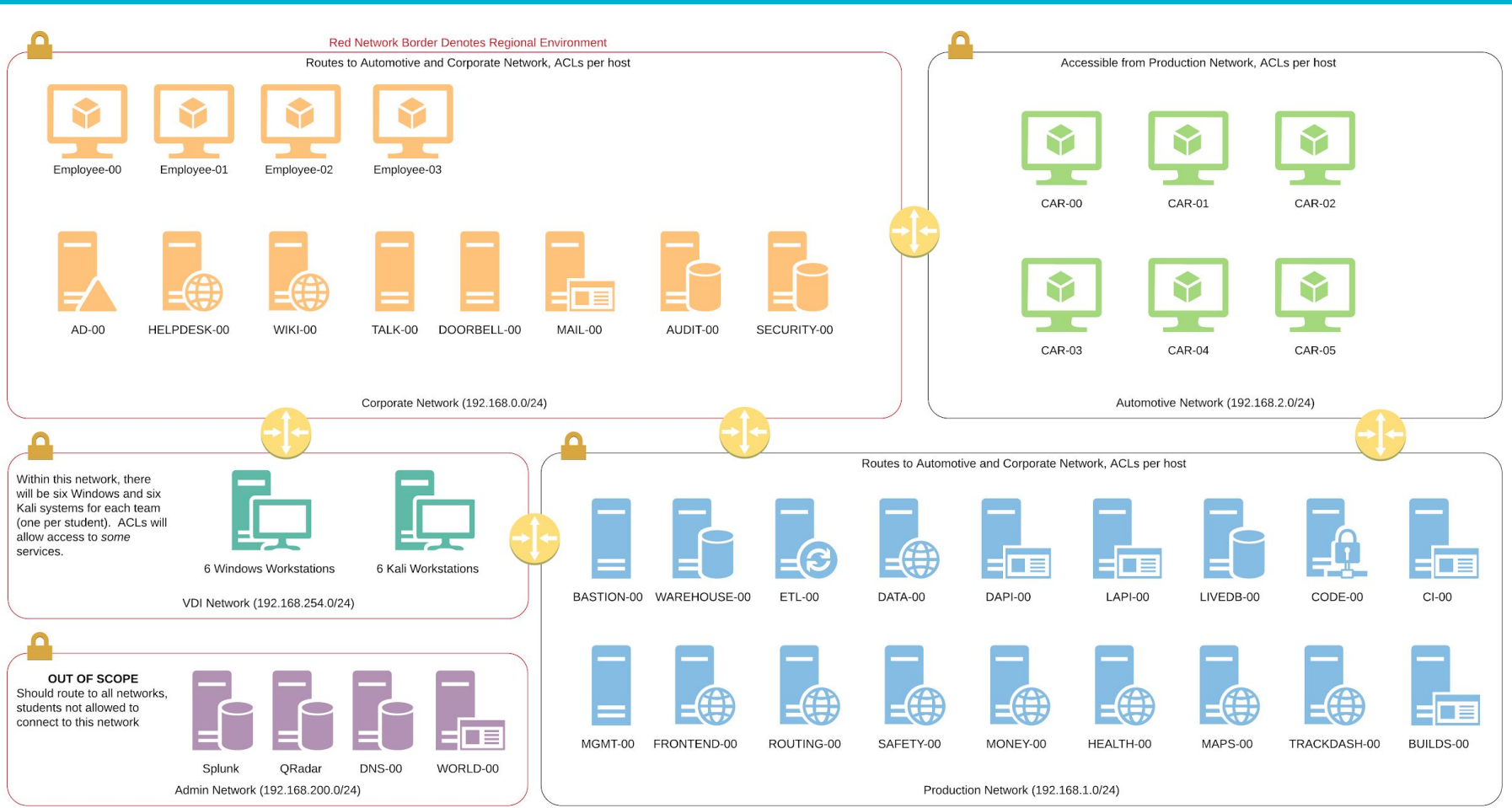
18 custom applications and libraries

Feature complete documentation

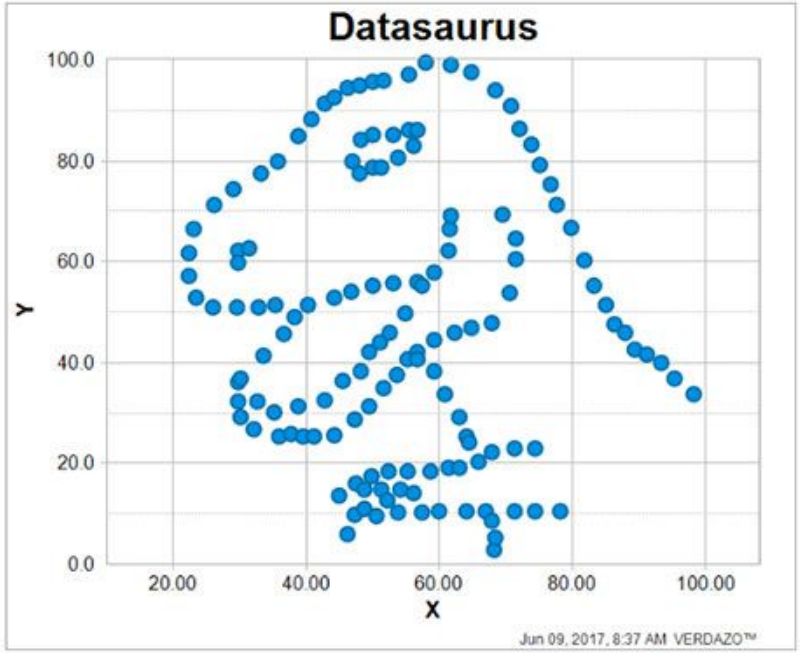
332 commits






Red Network Border Denotes Regional Environment
Routes to Automotive and Corporate Network, ACLs per host
Employee-00
Employee-01
Employee-02
Employee-03
AD-00
HELPDESK-00
WIKI-00
TALK-00
DOORBELL-00
MAIL-00
AUDIT-00
SECURITY-00
Corporate Network (192.168.0.0/24)
Accessible from Production Network, ACLs per host
CAR-00
CAR-01
CAR-02
CAR-03
CAR-04
CAR-05
Automotive Network (192.168.2.0/24)
Within this network, there will be six Windows and six Kali systems for each team (one per student). ACLs will allow access to *some* services.
6 Windows Workstations
6 Kali Workstations
VDI Network (192.168.254.0/24)
OUT OF SCOPE
Should route to all networks, students not allowed to connect to this network
Splunk
QRadar
DNS-00
WORLD-00
Admin Network (192.168.200.0/24)
Routes to Automotive and Corporate Network, ACLs per host
BASTION-00
WAREHOUSE-00
ETL-00
DATA-00
DAPI-00
LAPI-00
LIVEDB-00
CODE-00
CI-00
MGMT-00
FRONTEND-00
ROUTING-00
SAFETY-00
MONEY-00
HEALTH-00
MAPS-00
TRACKDASH-00
BUILDS-00
Production Network (192.168.1.0/24)

Statistics


Datasaurus
100.0
80.0
60.0
40.0
20.0
0.0
Y
20.00
40.00
60.00
80.00
100.00
X
Jun 09, 2017, 8:37 AM VERDAZO™

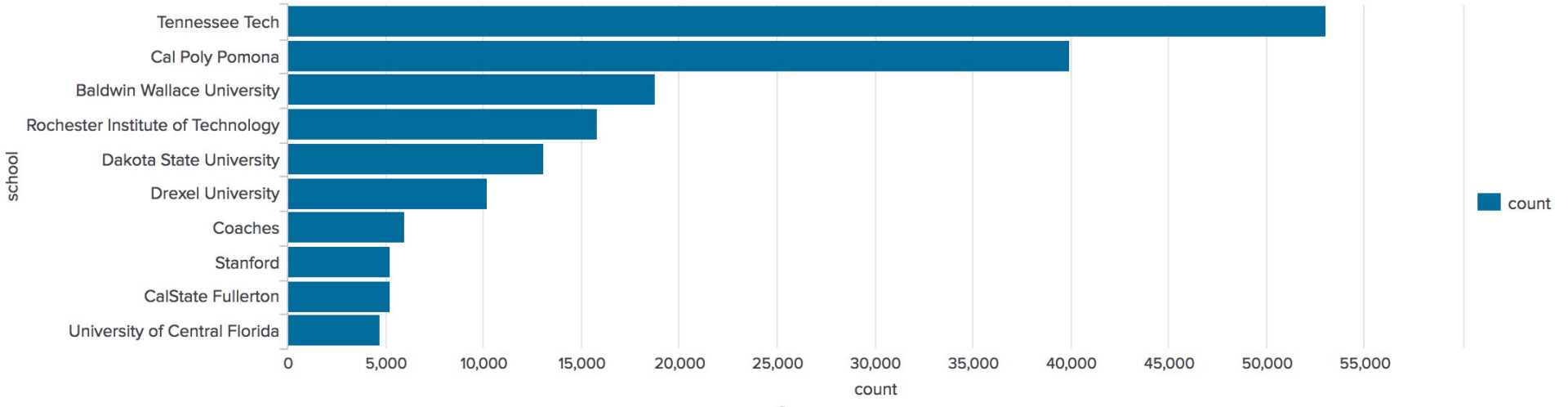
```
index=ids sourcetype="suricata:alert" NOT dest_ip="169.254.169.254" | stats count by school | sort - count
```

Date time range

✓ 172,273 events (11/3/18 9:00:00.000 AM to 11/3/18 7:30:00.000 PM) No Event Sampling Job Fast Mode

Events Patterns Statistics (10) **Visualization**

Bar Chart Format Trellis



```
sourcetype="suricata:alert" NOT dest_ip=169.254.169.254 | timechart count(alert.signature) by school
```

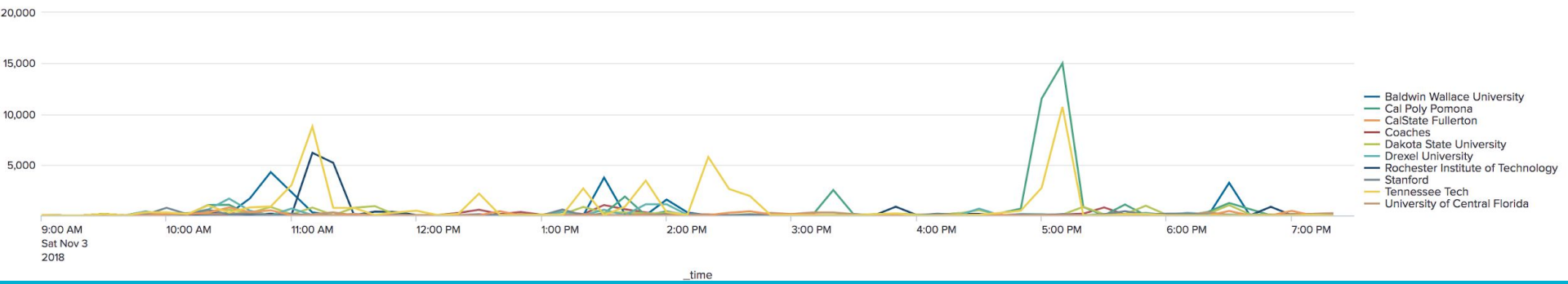
Date time range

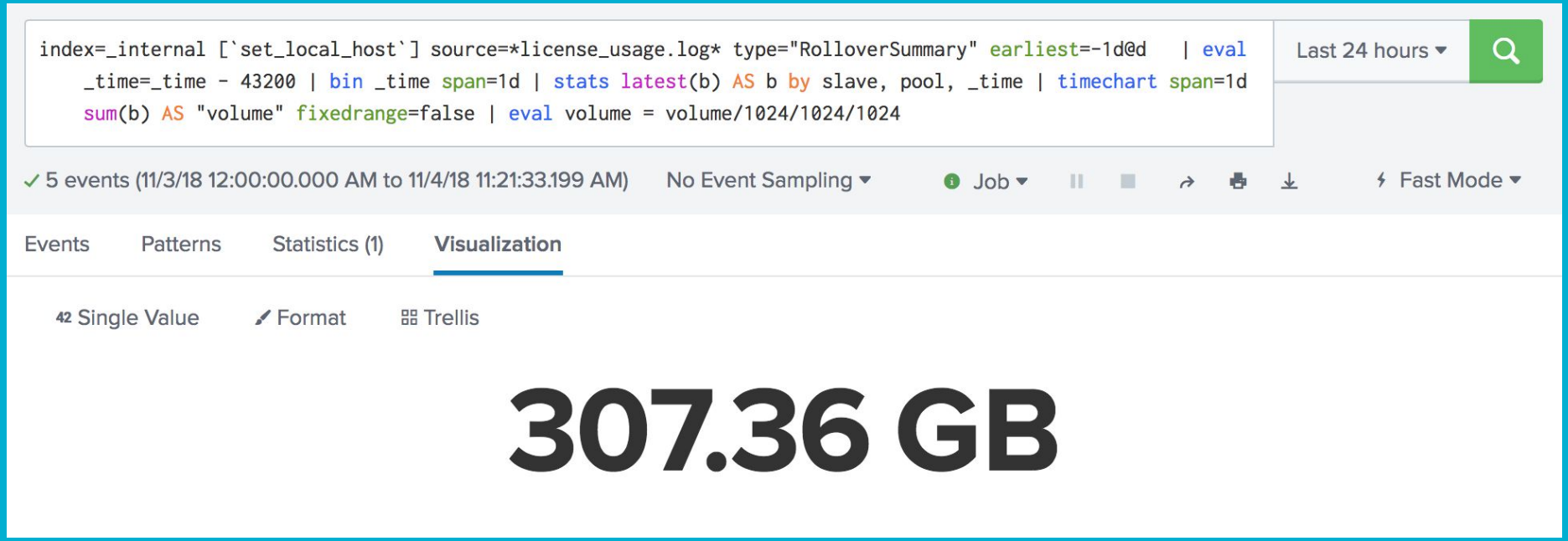
✓ 172,273 events (11/3/18 9:00:00.000 AM to 11/3/18 7:30:00.000 PM) No Event Sampling

Job Smart Mode

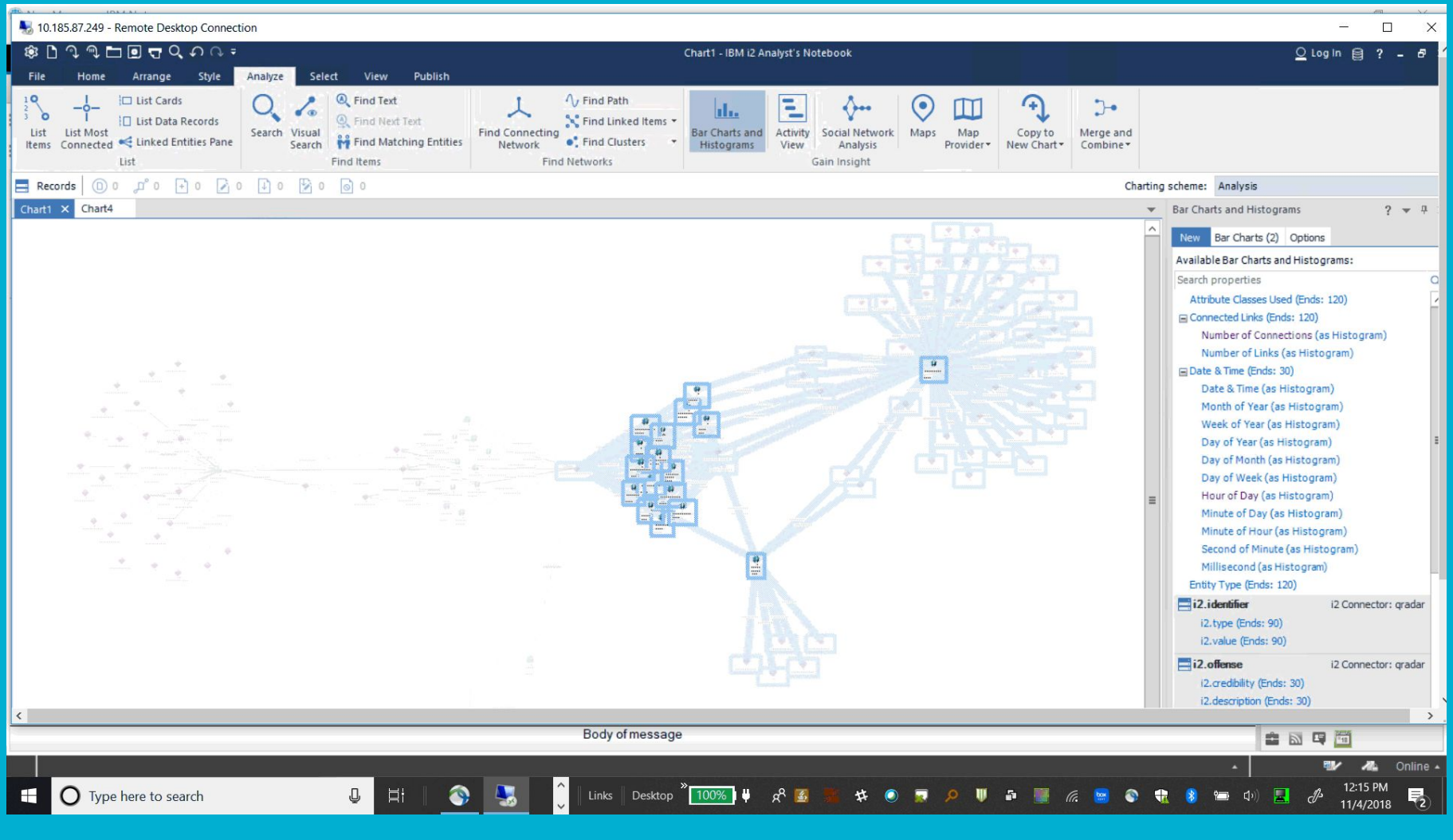
Events Patterns Statistics (63) Visualization

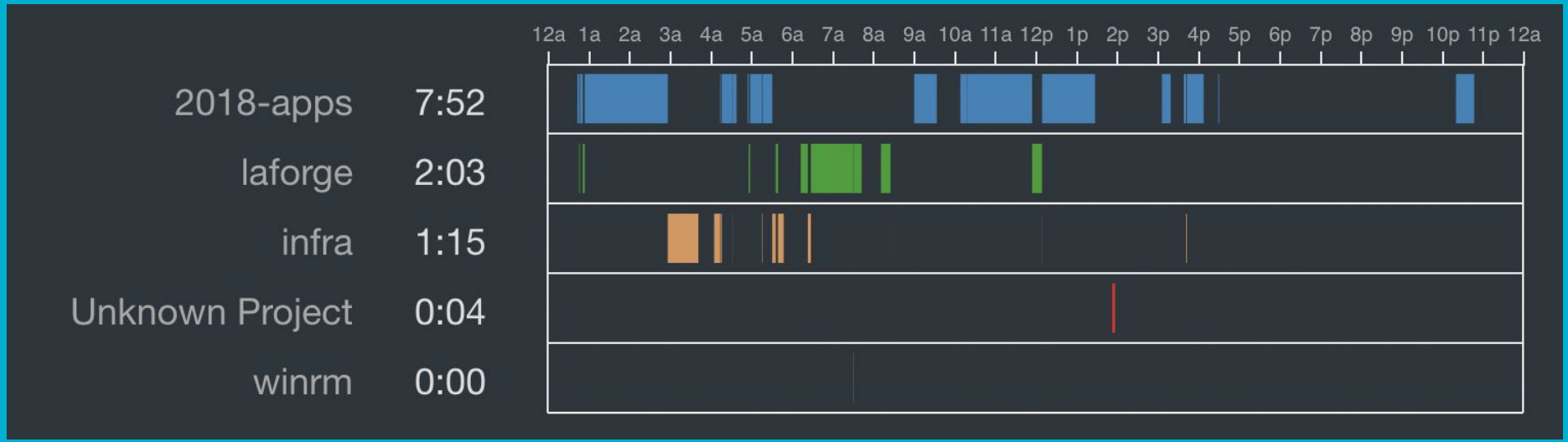
Line Chart Format Trellis




index=_internal [`set_local_host`] source=*license_usage.log* type="RolloverSummary" earliest=-1d@d | eval _time=_time - 43200 | bin _time span=1d | stats latest(b) AS b by slave, pool, _time | timechart span=1d sum(b) AS "volume" fixedrange=false | eval volume = volume/1024/1024/1024
Last 24 hours
✓ 5 events (11/3/18 12:00:00.000 AM to 11/4/18 11:21:33.199 AM)
No Event Sampling
Job
Fast Mode
Events
Patterns
Statistics (1)
Visualization
42 Single Value
Format
Trellis
307.36 GB

ls	3127	13.435593
clear	866	3.720890
cd ..	693	2.977572
exit	469	2.015124
ls -la	356	1.529604
ls -al	160	0.687462
ls -l	148	0.635903
cd	115	0.494114
ls -a	86	0.369511
ifconfig	80	0.343731


10.185.87.249 - Remote Desktop Connection
Chart1 - IBM i2 Analyst's Notebook
Log In
File
Home
Arrange
Style
Analyze
Select
View
Publish
List Items
List Most Connected
List Cards
List Data Records
Linked Entities Pane
List
Search
Visual Search
Find Text
Find Next Text
Find Matching Entities
Find Items
Find Connecting Network
Find Path
Find Linked Items
Find Clusters
Find Networks
Bar Charts and Histograms
Activity View
Social Network Analysis
Maps
Map Provider
Gain Insight
Copy to New Chart
Merge and Combine
Records
Charting scheme:
Analysis
Chart1
Chart4
Bar Charts and Histograms
New
Bar Charts (2)
Options
Available Bar Charts and Histograms:
Search properties
Attribute Classes Used (Ends: 120)
Connected Links (Ends: 120)
Number of Connections (as Histogram)
Number of Links (as Histogram)
Date & Time (Ends: 30)
Date & Time (as Histogram)
Month of Year (as Histogram)
Week of Year (as Histogram)
Day of Year (as Histogram)
Day of Month (as Histogram)
Day of Week (as Histogram)
Hour of Day (as Histogram)
Minute of Day (as Histogram)
Minute of Hour (as Histogram)
Second of Minute (as Histogram)
Millisecond (as Histogram)
Entity Type (Ends: 120)
i2.identifier
i2 Connector: qradar
i2.type (Ends: 90)
i2.value (Ends: 90)
i2.offense
i2 Connector: qradar
i2.credibility (Ends: 30)
i2.description (Ends: 30)
Body of message
Online
Type here to search
Links
Desktop
100%
12:15 PM
11/4/2018


12a 1a 2a 3a 4a 5a 6a 7a 8a 9a 10a 11a 12p 1p 2p 3p 4p 5p 6p 7p 8p 9p 10p 11p 12a
2018-apps 7:52
laforge 2:03
infra 1:15
Unknown Project 0:04
winrm 0:00


Family Photos

```
sourcetype="stream:dns" NOT query=*game.nationalcptc.org NOT query=*.wheelzapp.com | top query limit=20
```

Date time range

✓ 3,884,135 events (11/3/18 9:00:00.000 AM to 11/3/18 7:30:00.000 PM) No Event Sampling

Job Smart Mode

Events Patterns **Statistics (20)** Visualization

100 Per Page Format Preview

query	count	percent
localhost.google.internal	459518	24.605036
localhost.c.security-competitions.internal	459282	24.592400
wheelzapp.com	77128	4.129843
browserchannel-sites.l.google.com	43270	2.316906
www.google.com	21306	1.140836
nationalcptc.org	20384	1.091468
clients.l.google.com	16902	0.905023
version.bind	14203	0.760504
cello.client-channel.google.com	13902	0.744387
docs.google.com	12579	0.673547
ssl.gstatic.com	10757	0.575987
FHEPFCELEHFCEPFFFACACACACACACABM	10370	0.555265
org	9848	0.527314
play.google.com	9621	0.515159
clients6.google.com	9216	0.493474
clients4.google.com	8834	0.473019
0.docs.google.com	8692	0.465416
2.docs.google.com	8372	0.448281
a1089.dscd.akamai.net	7470	0.399984
api.snapcraft.io	7261	0.388793

```
sourcetype="stream:dns" NOT query=*game.nationalcptc.org NOT query=*.wheelzapp.com | top query limit=20
```

Date time range

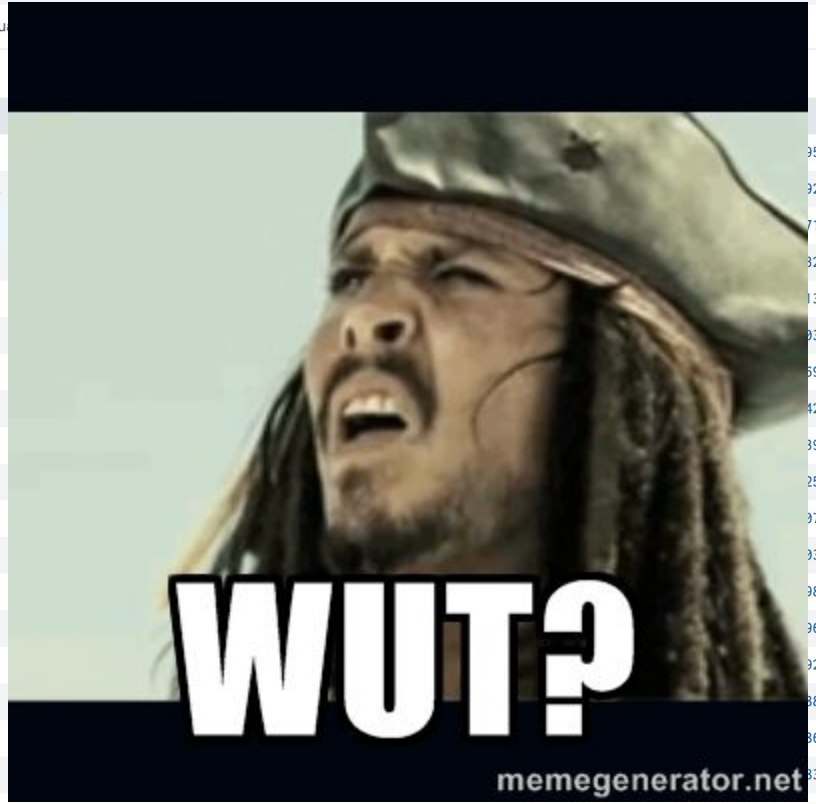
✓ 3,884,135 events (11/3/18 9:00:00.000 AM to 11/3/18 7:30:00.000 PM) No Event Sampling

Job Smart Mode

Events Patterns **Statistics (20)** Visu

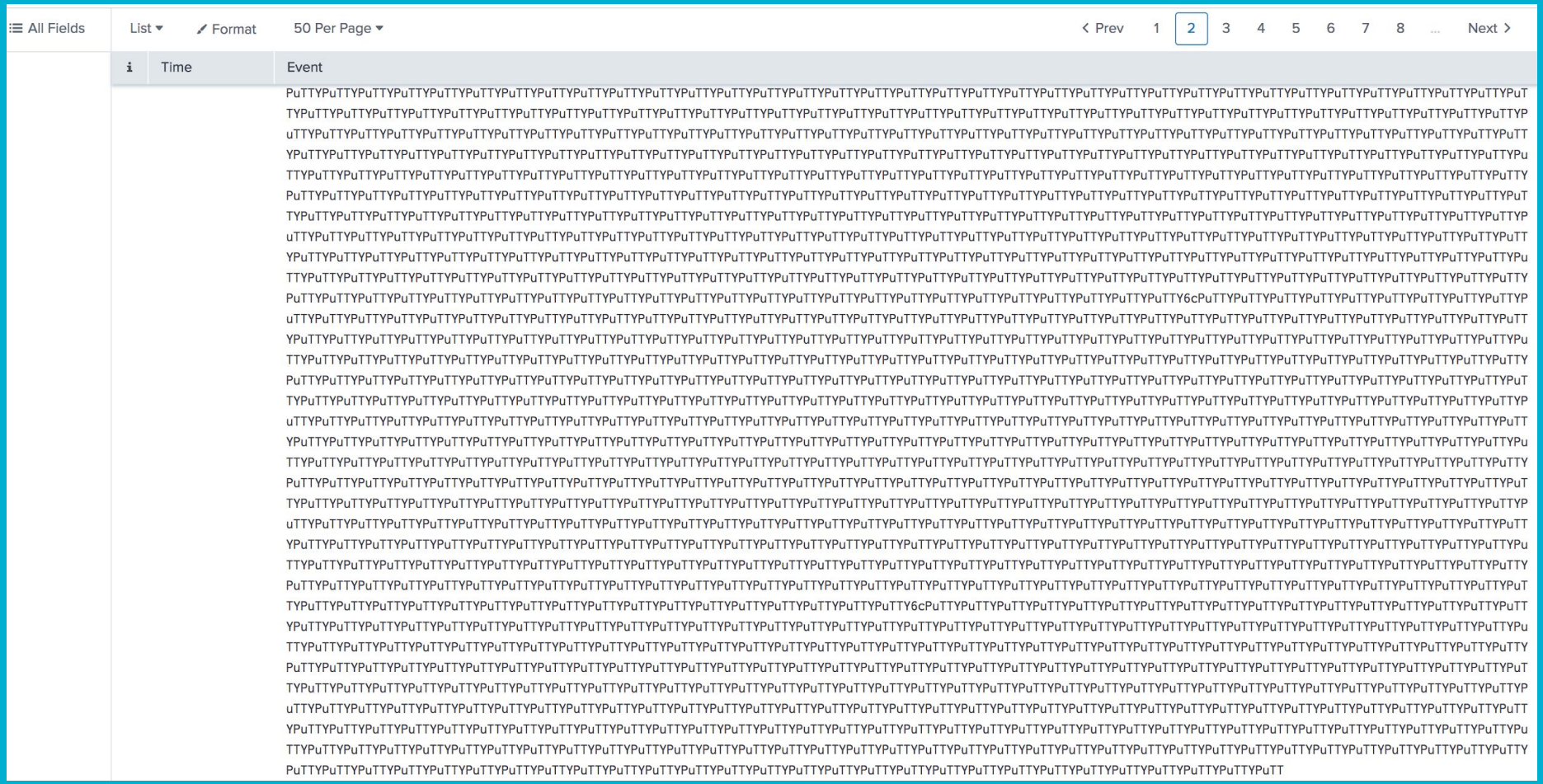
100 Per Page Format Preview

query		percent
localhost.google.internal	9518	24.605036
localhost.c.security-competitions.internal	9282	24.592400
wheelzapp.com	7128	4.129843
browserchannel-sites.l.google.com	3270	2.316906
www.google.com	1306	1.140836
nationalcptc.org	0384	1.091468
clients.l.google.com	6902	0.905023
version.bind	4203	0.760504
cello.client-channel.google.com	3902	0.744387
docs.google.com	2579	0.673547
ssl.gstatic.com	0757	0.575987
FHEPFCELEHFCEPFFFACACACACACACABM	0370	0.555265
org	9848	0.527314
play.google.com	0621	0.515159
clients6.google.com	9216	0.493474
clients4.google.com	8834	0.473019
0.docs.google.com	8692	0.465416
2.docs.google.com	8372	0.448281
a1089.dscd.akamai.net	7470	0.399984
api.snapcraft.io	7261	0.388793



beer.com	841	0.072454
paypal.com	758	0.065303
ebay.com	757	0.065217
facebook.github.io	5	0.000464
fastandeasyhacking.com	5	0.000464
firstimpression.io	5	0.000464

```
nmap -T4 -sV --script vuln,default -vv -p - -oA prod 10.0.2.0/24
```


All Fields
List
Format
50 Per Page
Prev
1
2
3
4
5
6
7
8
...
Next
Time
Event

```
index=os sourcetype=bash_history
| table _time bash_command
```

✓ 46 events (11/3/18 1:40:27.000 PM to 11/3/18 1:40:30.000 PM) No Event Sampling

Events (46) Patterns **Statistics (46)** Visualization

100 Per Page Format Preview

_time	bash_command
2018-11-03 13:40:27	-----BEGIN OPENSSH PRIVATE KEY-----
2018-11-03 13:40:27	5UixLw3X08Da1j3BKAlHPNZVLBGZuHiieT08bTOEhwxg/5tONXauyRmT5giOq7pIjZ1vLA
2018-11-03 13:40:27	9vDUyF4oQR4xd/qjQ2wvyTiFpkuOoTZzfIEaYoPeN3TX0QH/EAAACBAMkgSTbQLAB28bW+
2018-11-03 13:40:27	57/mh3z1IYS6hsIEZp2avNjyqLxj/u5z+Jwv6lFEwWuBV1LRStZQq5Jjqv0Xt/XdaMvO1I
2018-11-03 13:40:27	ALaXfTSe4AaAAAAIEA567cPnAnXdJMrACOAe7Q9jj2mbtwPazZDhv2Miu4/ZDIcgZHZwVQ
2018-11-03 13:40:27	Ah0jFEJEtQ0ymX69H6lstYQ3iXWW0ZkQlkLuN5GkKU6UQMunrX1tee7Jy3qiC9wt+W6Oly
2018-11-03 13:40:27	Bi/+w4sM218A35H6PXJlzb+tMDGhZdzEd2fuhDu4yiTo5Z/p5Q30X1rqsh7CaHxG3GdEE2
2018-11-03 13:40:27	CclwHIHKJvJEs7zg+mBM5R9prZ+s8IqDmfbvnvi9/f5G8SbErH59Nccu+3idF10QjV+I+p
2018-11-03 13:40:27	DGD/m041dq7JGZPmCI6rukiNnW8sCSPxelvhL5HBMh1wL3tdCXuPBAT4XbpjlkwZsXp4NN
2018-11-03 13:40:27	NhAAAAAwEAAQAAAQEAtgWDCwXzFij1wEPhWwUQIfMIc3e3EZN9mbWaYZJlHxqq0cNWBPxO
2018-11-03 13:40:27	PZkJphMbcGq+UwhRAAAAHXJvb3RAa2FsaTAxLnZkaS53aGVlbHphcHAuY29tAQIDBAU=
2018-11-03 13:40:27	UXEYORTZ6OSNRTCCbc8FhOdT6icXwbYZqQJ8aUov9338rMDGZJG41kPf6GvDCc1fQ44wN/
2018-11-03 13:40:27	b+krtwu5J1mRD5X+kIHZRQv9MngThV5oB+Mr4dkBwiUBAAAAgQCW1lnLeiJsWYASf8+HeA

You may lose your paycheck! Inbox ×

Wheelz Payroll Staff <wheelzhr@gmail.com> Don't trust emails just because they include the company name somewhere

to me

Generic greetings are a warning sign

Sir/Ma'am,

Your paycheck jepordy! Watch for typos like this one. They usually mean an email is unofficial

If you do not connect to the new HR site within 48 hours, you will not be included in the new payroll system database.

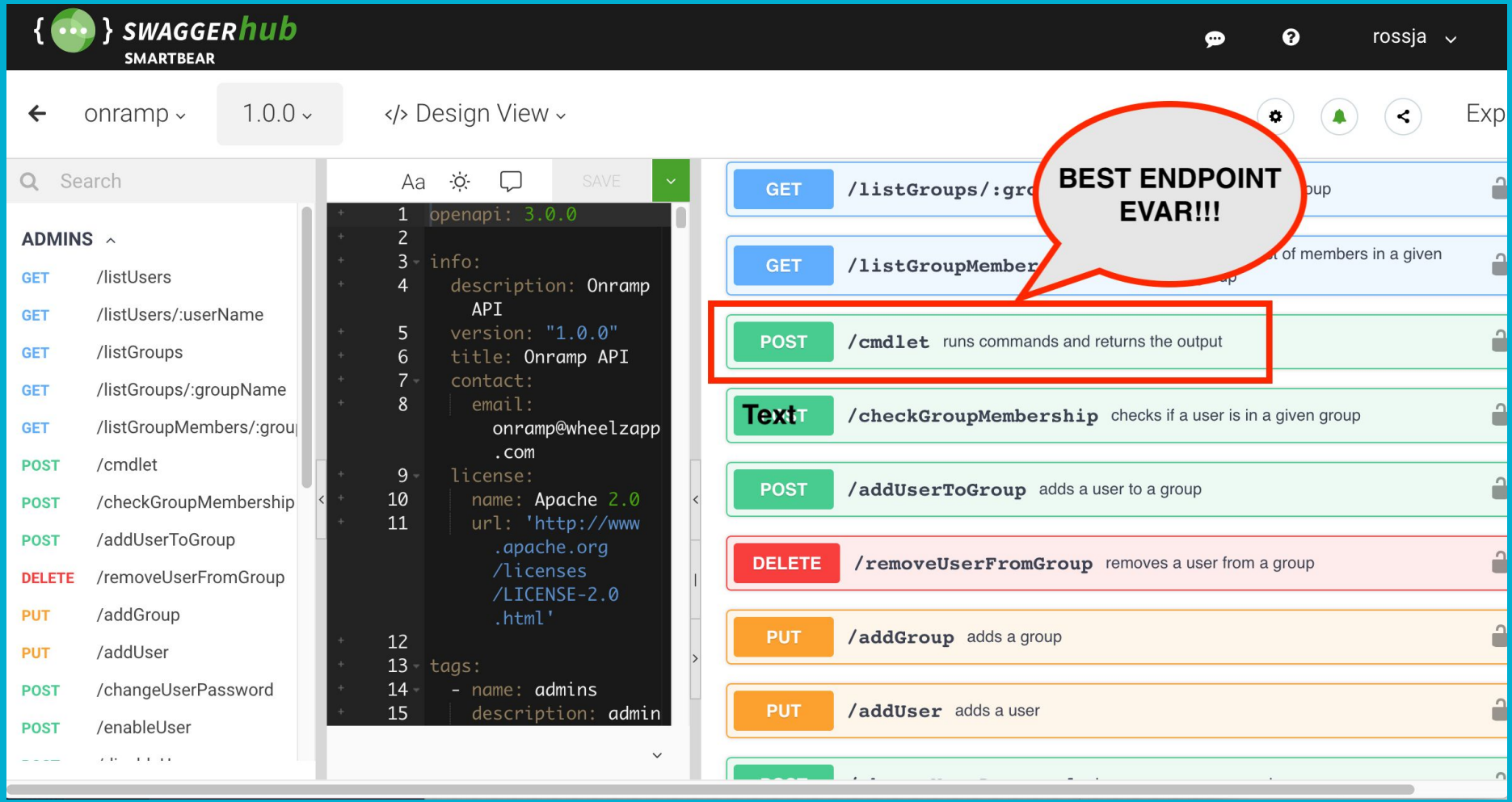
Please log in to the portal at http://wheelzapp.com/hr/payroll to register for the new database and get your check.

Actually links to http://87yao87y254o2h3ru89d7h8o4lef.ru/

Respectfully,

Payroll Team

This logo was ripped from github


SWAGGERhub
SMARTBEAR
rossja
onramp
1.0.0
Design View
Exp
Search
ADMINS
GET /listUsers
GET /listUsers/:userName
GET /listGroups
GET /listGroups/:groupName
GET /listGroupMembers/:grou
POST /cmdlet
POST /checkGroupMembership
POST /addUserToGroup
DELETE /removeUserFromGroup
PUT /addGroup
PUT /addUser
POST /changeUserPassword
POST /enableUser
Aa
SAVE
1 openapi: 3.0.0
2
3 info:
4 description: Onramp API
5 version: "1.0.0"
6 title: Onramp API
7 contact:
8 email: onramp@wheelzapp.com
9 license:
10 name: Apache 2.0
11 url: 'http://www.apache.org/licenses/LICENSE-2.0.html'
12
13 tags:
14 - name: admins
15 description: admin
GET /listGroups/:gro
GET /listGroupMember
BEST ENDPOINT EVAR!!!
POST /cmdlet runs commands and returns the output
Text
/checkGroupMembership checks if a user is in a given group
POST /addUserToGroup adds a user to a group
DELETE /removeUserFromGroup removes a user from a group
PUT /addGroup adds a group
PUT /addUser adds a user

```
index=os sourcetype=bash_history source="/home/jerrold.reddick/.bash_history" host="t8-corp-talk-00" "gcc" OR ".c" OR "a.out" OR "ohno" OR "exploit" OR "nice"
| table _time user_name bash_command
```

✓ 12 events (11/3/18 1:00:00.000 PM to 11/4/18 12:00:00.000 AM) No Event Sampling ▾ Job ▾

Events (12) Patterns **Statistics (12)** Visualization

100 Per Page ▾ Format Preview ▾

_time ▲	user_name	bash_command
2018-11-03 13:20:45	jerrold.reddick	./a.out
2018-11-03 13:20:45	jerrold.reddick	gcc exploit.c
2018-11-03 13:20:45	jerrold.reddick	vim exploit.c
2018-11-03 13:21:41	jerrold.reddick	gcc -o ohno ohno.c
2018-11-03 13:21:41	jerrold.reddick	vi ohno.c
2018-11-03 13:21:41	jerrold.reddick	./exploit
2018-11-03 13:21:41	jerrold.reddick	gcc -o exploit exploit.c
2018-11-03 13:21:41	jerrold.reddick	gcc exploit.c
2018-11-03 13:21:41	jerrold.reddick	gcc nice.c
2018-11-03 13:21:41	jerrold.reddick	vi nice.c
2018-11-03 13:30:02	jerrold.reddick	cat exploit
2018-11-03 14:11:23	jerrold.reddick	rm a.out exploit* nice.c ohno.c

Snacks


HIM? NO, HE DOESN'T WANT A COOKIE
HE SAYS I CAN HAVE TWO
WeKnowMemes

Created by George

Insider Threat

Ingredients:

Two Great Experts
(Plus a Chief Snacking Officer)

A REAL Remote Access Trojan

Emails, Pictures, and OSINT,
Oh my!

Steganography?

Methods:

Suspects

Process

Findings

Lineup

Snacks…?

Final Thoughts and Feedback

Understand the motivations of key players

Understand Risk (Likelihood * Impact)

Have a communication strategy

Slow down as you speak

Know your audience

Language is a powerful tool - use it appropriately