My Busman's Holiday
Using Splunk for Home IoT Baselining

bus·man's holiday [*noun*] \ ˈbəs-mənz- \ ˈhä-lə-ˌdā
: a holiday spent in following or observing the practice of one's usual occupation

James Callahan
(JP)

UScontracting Inc.

https://www.uscontractinginc.com/

Disclaimer

Please read the disclaimer carefully before you continue to view this presentation. I'm only going to give you less than 5 seconds, so I hope you can read fast. By attending this presentation, or viewing the saved version online later, you agree to the Terms of Use when this option is made available to you, you accept and agree to be bound and abide by the disclaimer. If you do not want to agree to this disclaimer, feel free to leave. Although no refunds will be issued, and you might hurt my feelings. All opinions and comments are the opinions and comments of the presenter and the inclusion in this presentation is in no way to be construed as or imply any endorsement or affiliation with his employer or any client organizations past, present or future. The information contained on this presentation and the resources linked through this presentation are for educational and informational purposes only. Your viewing of this presentation – including implementation of any suggestions set out in this presentation and/or use of any resources available on this presentation – does not create a professional-client relationship between you and me or my current past or future employers or client organizations. By using the information in this presentation, you accept personal responsibility for the results of your actions. You agree to take full responsibility for any harm or damage you suffer as a result of the use, or non-use, of the information available to you in this presentation or the resources available for download discussed in this presentation. You agree to use judgment and conduct due diligence before taking any action or implementing any of the items in this presentation. THE PRESENTER IS ABSOLVED OF ANY AND ALL LIABILITY OR LOSS THAT YOU OR ANY PERSON OR ENTITY ASSOCIATED WITH YOU MAY SUFFER OR INCUR AS A RESULT OF USE OF THE INFORMATION CONTAINED IN THIS PRESENTATION AND/OR THE RESOURCES YOU MAY DOWNLOAD FROM THAT ARE MENTIONED HEREIN. THE PRESENTER SHALL NOT BE LIABLE TO YOU FOR ANY TYPE OF DAMAGES, INCLUDING DIRECT, INDIRECT, SPECIAL, INCIDENTAL, EQUITABLE, OR CONSEQUENTIAL LOSS OR DAMAGES FOR USE OF ANY OF THE INFOMATION PRESENTED. THE INFORMATION, SOFTWARE, PRODUCTS, AND SERVICES DISCUSSED MAY INCLUDE INACCURACIES OR TYPOGRAPHICAL ERRORS. YOU CAN EXPECT THIS FROM THE PRESENTER, AS HIS BRAIN MOVES SLOWER THAN HIS FINGERS TYPES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PRESENTER BE LIABLE FOR ANY DIRECT, INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF USE, DATA OR PROFITS, ARISING OUT OF OR IN ANY WAY CONNECTED WITH THE USE OF THE INFOMRATION IN THIS PRESENTATION, WITH THE DELAY OR INABILITY TO USE INFORMATION, THE PROVISION OF OR FAILURE TO PROVIDE SERVICES, OR FOR ANY INFORMATION, SOFTWARE, PRODUCTS, SERVICES AND RELATED GRAPHICS OBTAINED THROUGH THE PRESENTATION, OR OTHERWISE ARISING OUT OF THE USE OF THE INFOMRATION IN THIS PRESENTATION, WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, EVEN IF THE PRESENTOR HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. BECAUSE SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. IF YOU ARE DISSATISFIED WITH ANY PORTION OF THE PRESENTATION, OR WITH ANY OF THESE TERMS OF USE, YOUR SOLE AND EXCLUSIVE REMEDY IS TO USE THE MEN IN BLACK'S NEURALIZER (THE FLASHY THING) TO ERASE THIS HORRIBLE MEMORY.

Disclaimer

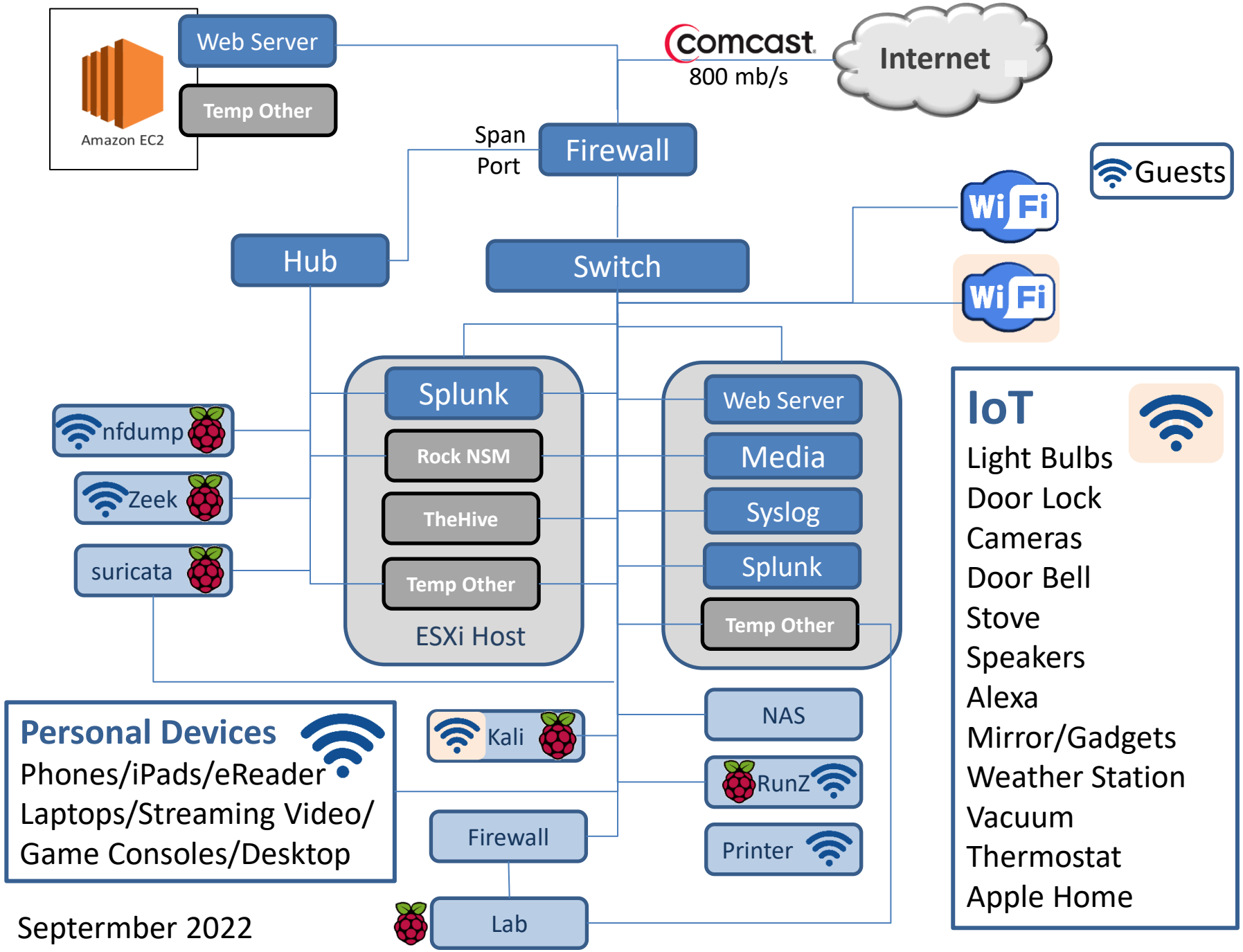
Please read the disclaimer carefully before you continue to view this presentation. I'm only going to give you less than 5 seconds, so I hope you can read fast. By attending this presentation, or viewing the saved version online later, you agree to the Terms of Use when this option is made available to you, you accept and agree to be bound and abide by the disclaimer. If you do not want to agree to this disclaimer, feel free to leave. Although no refunds will be issued, and you might hurt ns and comments are th pinions and comments of the presenter and the inclusion in this presentation is in no way t y endorsem his employer or any client organizations past, present or future. The information containe esourc tation are for educa ional purposes only. Your viewing of this prese ation c presentation a es available on this presentation – does not crea lations ent past or fu organizations. By using the information in this presenta ot person ur action Y responsibility for any harm or damage you suffer as a result of the use, on-us in this presentation or resources available for download discussed in this presentation. You agree to se ju efore taking any action or implementing any of the items in this presentation. THE PRESENTER IS ABSOLVED OF ANY A U OR ANY PERSON OR ENTITY ASSOCIATED WITH YOU MAY SUFFER OR INCUR AS A RESULT OF USE OF THE INFORMATIC N AND/OR THE RESOURCES YOU MAY DOWNLOAD FROM THAT ARE MENTIONED HEREIN. THE PRESENTER SHALL NOT F DAMAGES, INCLUDING DIRECT, INDIRECT, SPECIAL, INCIDENTAL, EQUITABLE, OR CONSEQUENTIAL LOSS OR DAM FOMATION PRESENTED. THE INFORMATION, SOFTWARE, PRODUCTS, AND SERVICES DISCUSSED MAY INCLUDE INACC ERRORS. YOU CAN EXPECT THIS FROM THE PRESENTER, AS HIS BRAIN MOVES SLOWER THAN HIS FINGERS TYPES. TO THE BY APPLICABLE LAW, IN NO EVENT SHALL THE PRESENTER BE LIABLE FOR ANY DIRECT, INDIRECT, PUNITIVE, IN ECIAL, AL ANY DAMAGES WHATSOEVER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF USE, DATA RISING OUT OF OR IN A CTED WITH THE USE OF THE INFOMRATION IN THIS PRESENTATION, WITH THE DELAY OR INABILITY IATION, THE PROVISIO TO PROVIDE SERVICES, OR FOR ANY INFORMATION, SOFTWARE, PRODUCTS, SERVI ED GRAPHICS OBTAINED PRESENTATION, OR OTHERWISE ARISING OUT OF THE USE OF THE INFOMRATION IN THIS PRESENTATION, WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, EVEN IF THE PRESENTOR H USION OR LIMITATION OF LIA ISSATISFIED WITH ANY PORTION OF THE PRESENTATION, OR WITH ANY OF THESE TERMS OF USE, YOUR SOLE AND EXCLUSIVE REMEDY IS TO USE THE MEN IN BLACK'S NEURALIZER (THE FLASHY THING) TO ERASE THIS HORRIBLE MEMORY.

Not representing my company or any client organizations

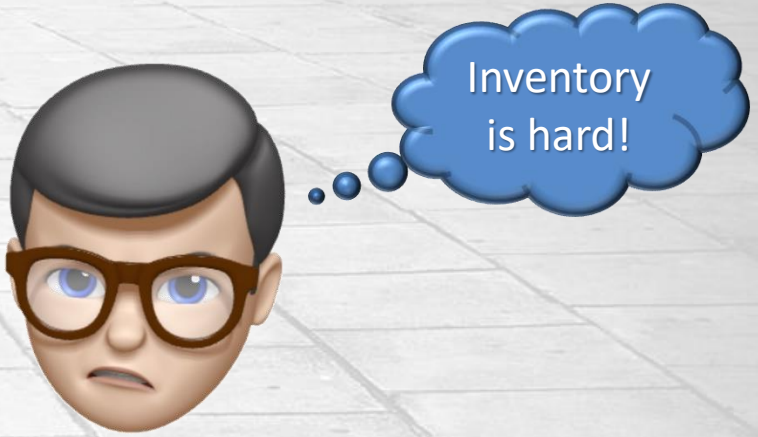
About JP

- Professional Paranoid
- Retired US Army CW4
- Computer Hobbyist
- Irish Band and Solo Artist
- ‘65 Mustang
- Not looking for a job

If you’re not having fun, you’re in the wrong line of work.


Amazon EC2
Web Server
Temp Other
comcast
800 mb/s
Internet
Span
Port
Firewall
Guests
Wi Fi
Wi Fi
Hub
Switch
Splunk
Rock NSM
TheHive
Temp Other
ESXi Host
Web Server
Media
Syslog
Splunk
Temp Other
nfdump
Zeek
suricata
IoT
Light Bulbs
Door Lock
Cameras
Door Bell
Stove
Speakers
Alexa
Mirror/Gadgets
Weather Station
Vacuum
Thermostat
Apple Home
Personal Devices
Phones/iPads/eReader
Laptops/Streaming Video/
Game Consoles/Desktop
Kali
NAS
RunZ
Printer
Firewall
Lab
Septermber 2022

Inventory



- Different methods yield differing results (by count)
- Not everything is online during snap shot sampling
- MAC OUI are not always helpful in figuring out what's what
- Outbound DNS can help with ID

Inventory Data Points
- MAC Address
- IP Address
- Client Name
- Type (IoT, personal device, VM, etc)
- Last Seen (_time)

```
|inputlookup inventory_all.csv
```

Local Inventory Counts

Knock-Knock, Who's there (or here)

IPs pinged **91** ↗ 4
compared to yesterday

MACs in Flow **110** → 0
compared to yesterday

Inventory of Inventory (Last 8 days Stored Inventory)

IPs	MACs	Client_Names
151	151	65

The Big Inventory List | Rumble Asset Review

```
(macs in flows -2d@d)

| tstats summariesonly=true allow_old_summaries=true
sum(All_Traffic.bytes) as bytes values(sourcetype) as sourcetype count from
datamodel="Network_Traffic"   groupby All_Traffic.src_ip, All_Traffic.src_mac
All_Traffic.dest_mac _time
| rename All_Traffic.* as *
| eval mac=src_mac+"|"+dest_mac
| makemv delim="|" mac
| mvexpand mac
| search mac!=33:33* mac!=FF:FF:FF*
| timechart dc(mac) as mac span=1d
```

DHCP Assignments

(dhcp range: .100 – .254)

Last 24h

last_seen	mac	ip	client
09/05/2022 01:10:50	88:71:e5:3a:77:f5	192.168.0.128	amazon-004efe015
09/05/2022 00:35:58	24:f5:a2:50:3b:15	192.168.0.129	wemo_front_door
09/05/2022 04:08:19	38:1a:52:03:f1:74	192.168.0.130	EPSON03F174
09/05/2022 02:38:30	00:17:88:25:cd:78	192.168.0.136	Philips-hue
09/05/2022 01:10:32	84:0d:8e:91:48:32	192.168.0.140	nexx_garage
09/05/2022 01:11:57	44:67:55:23:59:e4	192.168.0.144	espressif
09/05/2022 02:07:59	50:de:06:65:47:19	192.168.0.145	EntertamentRoom
09/05/2022 03:19:03	72:9b:0e:5f:67:b3	192.168.0.146	iphone
09/05/2022 03:50:40	90:70:65:62:f4:1c	192.168.0.154	lutron-031f3b00
09/05/2022 00:36:53	70:9c:d1:88:26:29	192.168.0.157	snazzy-blue-laptop

« Prev 1 2 3 4 5 6 Next »

Add MAC - Review List

57 DHCP Assignments -24h

Dashboard panels from Speakers Splunk landing page

Sep 2022

Splunk Asset Discovery App

Awesome App

Asset Discovery

Host Overview

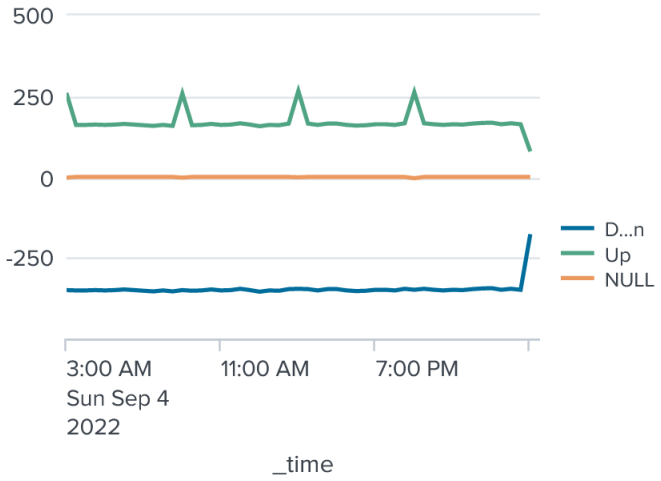
Distinct IPs available during timeframe: **91**

Asset State

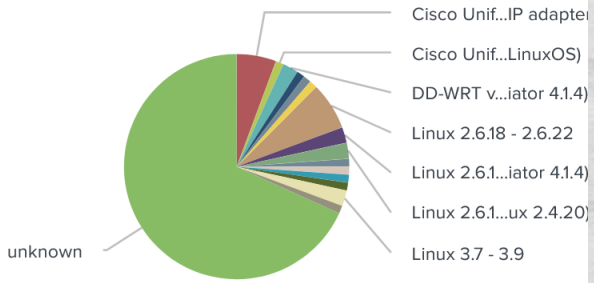
dest_ip	dest_host	status	minutes_ag
192.168.0.17	dublin	Up	1
192.168.0.20	lugh	Up	1
192.168.0.21	wx_splunk	Up	1
192.168.0.22	sisyphus	Up	1
192.168.0.23	freckles	Up	1

« Prev 1 2 3 4 5 6 7 8 9

Historical Availability



Operating System Signatures



Script input config

Command	Interval	Source type	App
/opt/splunk/etc/apps/asset_discovery/bin/nmap.sh	900	ping_scan	asset_discovery
/opt/splunk/etc/apps/asset_discovery/bin/nmap.sh -A -O	21600	port_scan	asset_discovery

Non-Splunk Inventory Product

- Splunk app for paying customers
  https://splunkbase.splunk.com/app/6549/
- Raw data API for those of us just dabbling

runZero

86 recent assets

77 live · 18 offline

www.runzero.com

Asset inventory

Search assets...

Save query | Copy query link | Reset filters

Cols

0 selected | Viewing 0 - 95 of 95 results | 100 results

Addresses	Up	Attrs	Hostname	OS	Type	Hardware	Outlier	MAC	MAC vendor
192.168.0.1 +1			PFSENSE-5EE38736AD57A +1	FreeBSD 12.2-STABLE	Firewall	PfSense Firewall	2	00:08:A2:0E:2B:92	ADI Engineerir
192.168.0.2			ATHRU	D-Link DGS-1210-52	Switch	D-Link DGS-1210-52	2	BC:22:28:0E:AE:93 +52	D-Link Interna
192.168.0.8			DDWRT_8	DD-WRT 12548M	Broadband Router		2	00:1A:70:3E:25:CE	Cisco-Linksys,
192.168.0.9			TIPPERARY +1	Linux	Device	Asus Device	1	7C:10:C9:73:54:48	ASUSTek COM
192.168.0.16 +1			LOCALHOST	VMware ESXi 6.7.0 build-8169922	Hypervisor		2	1C:1B:0D:EE:8A:B6	GIGA-BYTE TE
192.168.0.17 +5			DUBLIN +1	Microsoft Windows Server 2012	Desktop		2	70:54:D2:7C:5C:1C +1	PEGATRON CO
192.168.0.20 +1			LUGH	Ubuntu Linux 14.04	Server	VMware VM	2	00:0C:29:0F:DE:0D	VMware, Inc.
192.168.0.21				CentOS Linux 7	Server	VMware VM	1	00:0C:29:0B:AC:A6	VMware, Inc.
192.168.0.22 +1			SISYPHUS	Ubuntu Linux 14.04	Server	VMware VM	2	00:0C:29:BE:01:01	VMware, Inc.

```
[splunkuser@splunkhost]# rumble_get.sh
curl -H "Authorization: Bearer [api key]" https://console.rumble.run/api/v1.0/export/org/assets.csv > /opt/splunk/etc/apps/splunkapp/lookups/assets.csv
```

ping sweep -> arp -> csv

Experiment – not on cron schedule …yet?

```
|inputlookup inventory_splunkhost_arp2.csv
| append    [| inputlookup inventory_ splunkhost _nmap_mac.csv]
| eval mac=lower(if(mac="<incomplete>","<incomplete>"+ip,mac))
| dedup mac
```

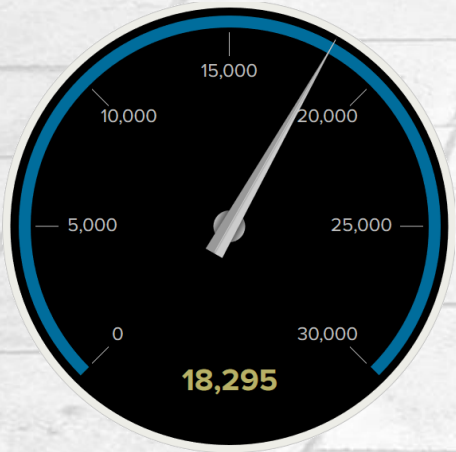
Combined, normalized & deduped - 101

```
[user@splunkhost ~]$ inventory_nmap_arp.sh
#
# jpcallahan professionalparanoid.com
#
nmap -sP 192.168.0.1-254 |grep MAC |sed 's/^/\n/;ta;:a;s/\n$//;t;/\n /{x;/./{x;s/\n /_\n/;ta};x;s/\n /
\n/;ta};/\n(/{x;s/^/x/;x;s/\n(/(\n/;ta};/\n)/{x;s/.//;x;s/\n)/)\n/;ta};s/\n\([^ ()]*\)/\1\n/;ta' |sed 's/MAC
Address\://g;s/\ /\,/g;s/\(Unknown\)//g;s/()//g;1i ip,mac,oui' > /opt/splunk/etc/apps/myapp/lookups/inventory_
splunkhost _nmap_mac.csv
#
#
#
arp -a |cut -d " " -f1,2,4 |sort |uniq |  /bin/sed 's/[(),]//g; s/\ /\,/g; s/\?//g;1i  client,ip,mac' >
/opt/splunk/etc/apps/myapp/lookups/inventory_ splunkhost _arp2.csv
```

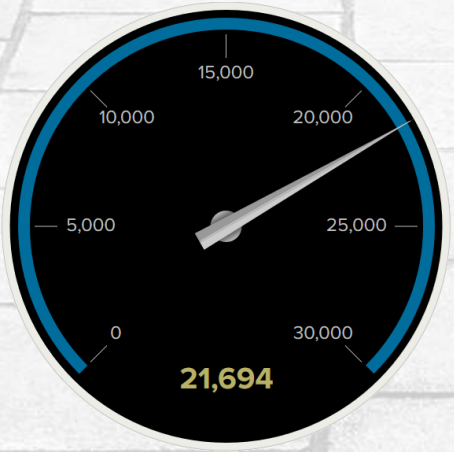
nmap MAC list - 78

arp MAC list - 91

Finding Anomalies

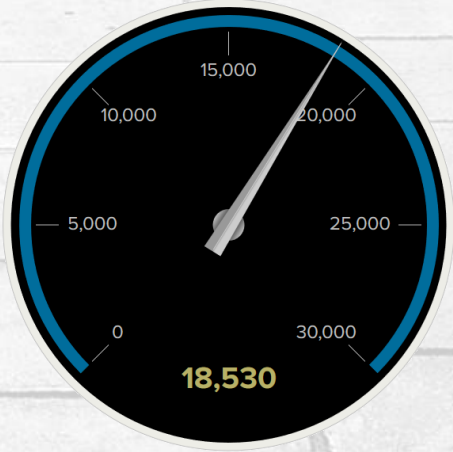


nfdump



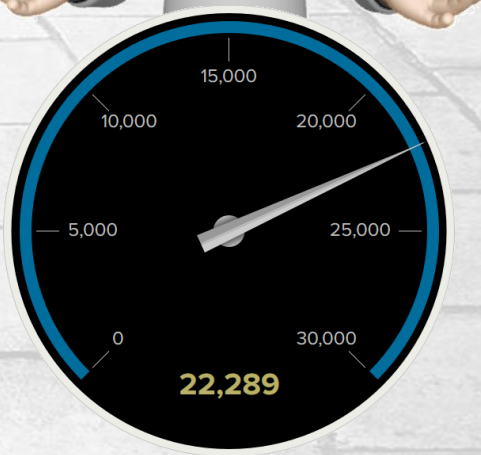
Zeek

dedup uid



Suricata

dedup flow_id



Stream App

dedup flow_id

netflow collected for the same 60 min time frame

Running four netflow collectors

IoT Baselining

- DNS and daily dest IP count for IoT (dns sec not an issue …yet)
- Experimenting with destination port assessments

New printer's first connections.

outbound_review

Looking at outcound traffic for the IoT stuff

Select System

Last 24 hours | EPSON03F174 | Hide Filters

2ndLevelDomainStats

In the time frame selected, 48 source IPs went to 676 second level domains after 86450 dns lookups for that(those) 2d level domain(s)
Filtered for host:EPSON03F174

twold	count	src_ip	client	src_ip_count	sparkline
epson.biz	3	192.168.0.130	EPSON03F174	1	
epson.net	3	192.168.0.130	EPSON03F174	1	

click for google search for epson.biz

Outbound DNS Query Review

outbound_review

Looking at outbound traffic for the IoT stuff

Select System: philips-hue

Select Type: *

And/Or Second Level Domain: *

multi-ip: filter out multi-ip

Last 4 hours

2ndLevelDomainStats

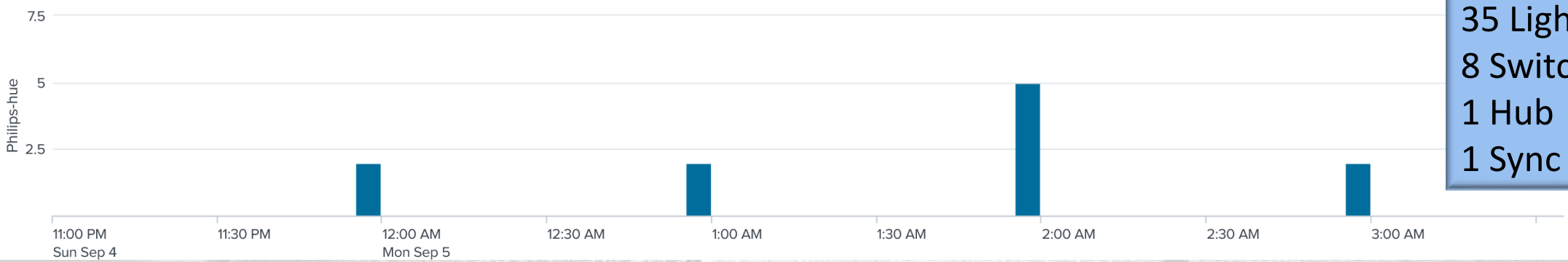
In the time frame selected, 64 source IPs went to 436 second level domains after 15833 dns lookups for that(those) 2d level domain(s)

Filtered for host:philips-hue and/or *

twold	count	src_ip	client	type	sparkline
ltsapis.goog	11	192.168.0.136	Philips-hue	iot_light	
meethue.com	786	192.168.0.128 192.168.0.136 192.168.0.226	amazon-004efe015 Philips-hue daddys-iPhone11	iot_alexa personal_dev	
philips.com	5	192.168.0.136	Philips-hue	iot_light	

click for google search for ltsapis.goog

chart for domain ltsapis.goog



Phillips Hue
35 Lights
8 Switches
1 Hub
1 Sync Box

Outbound DNS Query Compare

Systems Baseline

started 14 Aug 2021; Modified 4 Sep with IoT Only Check Box

Edit | Export | ...

Filter Type: iot_light ×

IoT Only: ☑ Only IoT

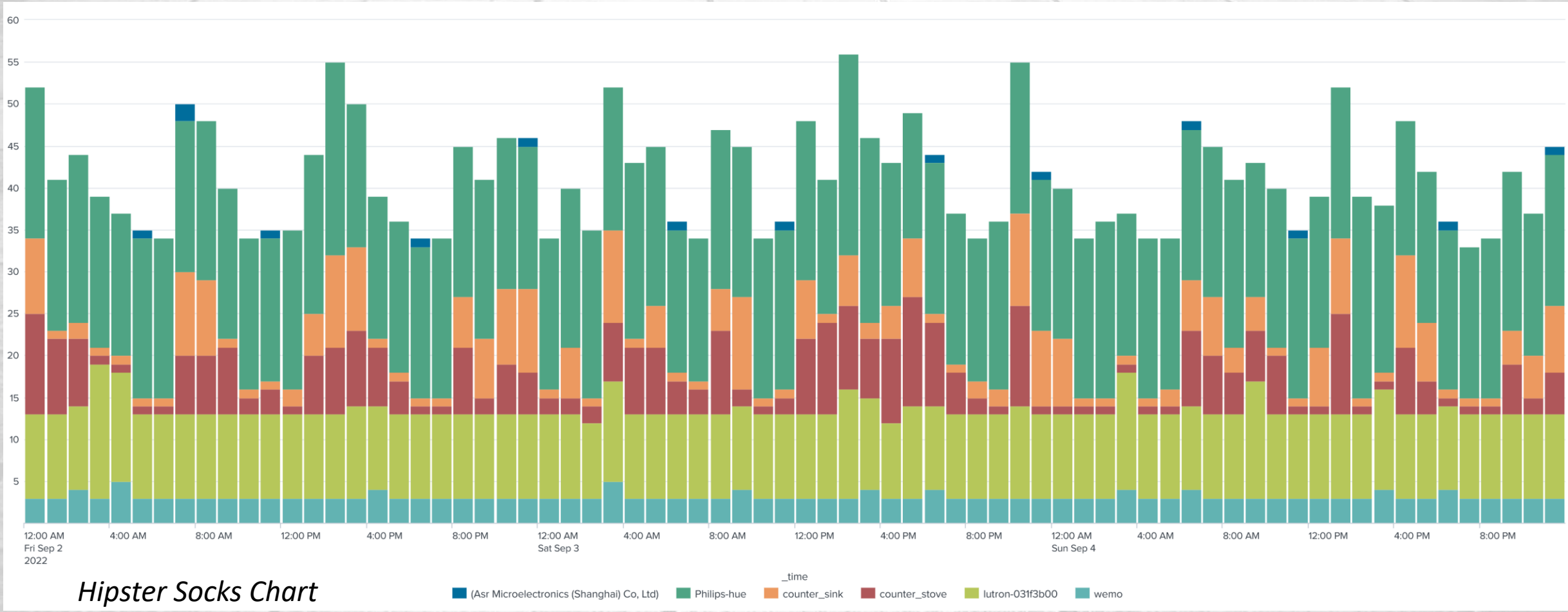
Hide Filters

Count of DNS domain query by day (3 day look back)
Red indicates a count change between days.

based on count of unique DNS 2d level domain queries filtered for type IN(iot_light) type=iot*

src_ip	day	Daily count of domains	client	type	Compare Counts
192.168.0.218	Friday	1	(Asr Microelectronics (Shanghai) Co, Ltd)	iot_light	1
192.168.0.136	Friday	3	Philips-hue	iot_light	1
192.168.0.136	Saturday	3	Philips-hue	iot_light	1
192.168.0.136	Sunday	3	Philips-hue	iot_light	1
192.168.0.250	Friday	1	counter_sink	iot_light	1
192.168.0.250	Saturday	1	counter_sink	iot_light	1
192.168.0.250	Sunday	1	counter_sink	iot_light	1
192.168.0.233	Friday	1	counter_stove	iot_light	1
192.168.0.233	Saturday	1	counter_stove	iot_light	1
192.168.0.233	Sunday	1	counter_stove	iot_light	1
192.168.0.154	Friday	4	lutron-031f3b00	iot_light	1
192.168.0.154	Saturday	5	lutron-031f3b00	iot_light	2
192.168.0.154	Sunday	4	lutron-031f3b00	iot_light	2

Outbound Dest IP Count Review



Hipster Socks Chart

Destination Port Baselining Experiment

client	0	123	443	53	67	80	Regisgtered	Rendom_High
(Asr Microelectronics (Shanghai) Co, Ltd)	52-icmp				2-udp 3-udp			
Philips-hue	909-icmp	122-udp	274-tcp	192-udp	2-udp	13-tcp	136-udp	46-udp
counter_sink	228-icmp		62-tcp	23-udp	2-udp		46-tcp	
counter_stove	241-icmp		57-tcp	34-udp	1-udp		3-udp 56-tcp	
lutron-031f3b00	604-icmp	49-udp	6-tcp	47-udp	2-udp	52-tcp	1-tcp 49-udp	
wemo_front_door	208-icmp	48-udp			3-udp		50-udp 72-tcp	

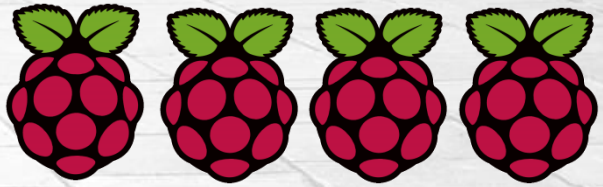

```
| tstats summariesonly=false allow_old_summaries=true count from datamodel=Network_Traffic where
All_Traffic.action!=blocked  AND All_Traffic.src=192.168.0.0/24 by All_Traffic.user All_Traffic.src All_Traffic.dest
All_Traffic.transport  All_Traffic.dest_port _time
| rename All_Traffic.* as *
| fillnull value="(unk)" protocol
| eval dpt_range=case(dest_port<1024,dest_port,dest_port<49151,"Regisgtered",1=1,"Rendom_High")
| eval transport=if(dest_port="0","icmp",transport)| stats values(dest_port) as dptv count by  src dpt_range transport
| eval proto_count=(count+"-"+transport)
| lookup mac_tracking.csv ip as src outputnew client type
| search  type=iot* type IN(iot_light)| sort + dptv
| chart values(proto_count)  by  client dpt_range limit=0
```

New E-Reader

twold	count	src_ip	client	sparkline
barnesandnoble.com	33	192.168.0.160	android-508cf9b73d1d9695	
crashlytics.com	1	192.168.0.160	android-508cf9b73d1d9695	
facebook.com	19	192.168.0.160	android-508cf9b73d1d9695	
facebook.net	1	192.168.0.160	android-508cf9b73d1d9695	
fbcdn.net	1	192.168.0.160	android-508cf9b73d1d9695	
gigya.com	4	192.168.0.160	android-508cf9b73d1d9695	
gstatic.com	18	192.168.0.160	android-508cf9b73d1d9695	
imagesbn.com	5	192.168.0.160	android-508cf9b73d1d9695	
localytics.com	29	192.168.0.160	android-508cf9b73d1d9695	
nook.com	48	192.168.0.160	android-508cf9b73d1d9695	
ntp.org	2	192.168.0.160	android-508cf9b73d1d9695	

…ThAt's a LoT of FaCebOOk foR a GaDgeT w/o a BrOwSer!

Use case: Baselining IoT
New Raspberry PI 4



Now, that's more like it…

twold	count	src_ip	client	sparkline
ntp.org	8	192.168.0.245 192.168.0.254	raspberrypi raspberrypi	
raspberrypi.org	21	192.168.0.245 192.168.0.254	raspberrypi raspberrypi	
realvnc.com	2	192.168.0.245	raspberrypi	
umd.edu	9	192.168.0.245 192.168.0.254	raspberrypi raspberrypi	

Splunk in home lab

- Running two different Splunk instances on VMs
- The Free license includes
  - **500 MB/day** of indexing volume and
    Now has no expiration date
  - Running in kiosk mode for magic mirror
- Splunk Developer/Developer Test
  - For internal, non-production use
  - Limited to 10 GB (Dev) or 50 GB (Dev/Test) per day
  - Good for six months, then can renew
  - Assigned to individuals, not organizations
  - Dev available to non-customers (prospects)

https://dev.splunk.com/enterprise/dev_license/
https://www.splunk.com/en_us/resources/personalized-dev-test-licenses.html

buh-bye…

Questions
Comments
Snide Remarks

some after bits

A few dashboards and other things:

https://github.com/azjimbo/

Other items available from

go SPLUNK

gosplunk.com