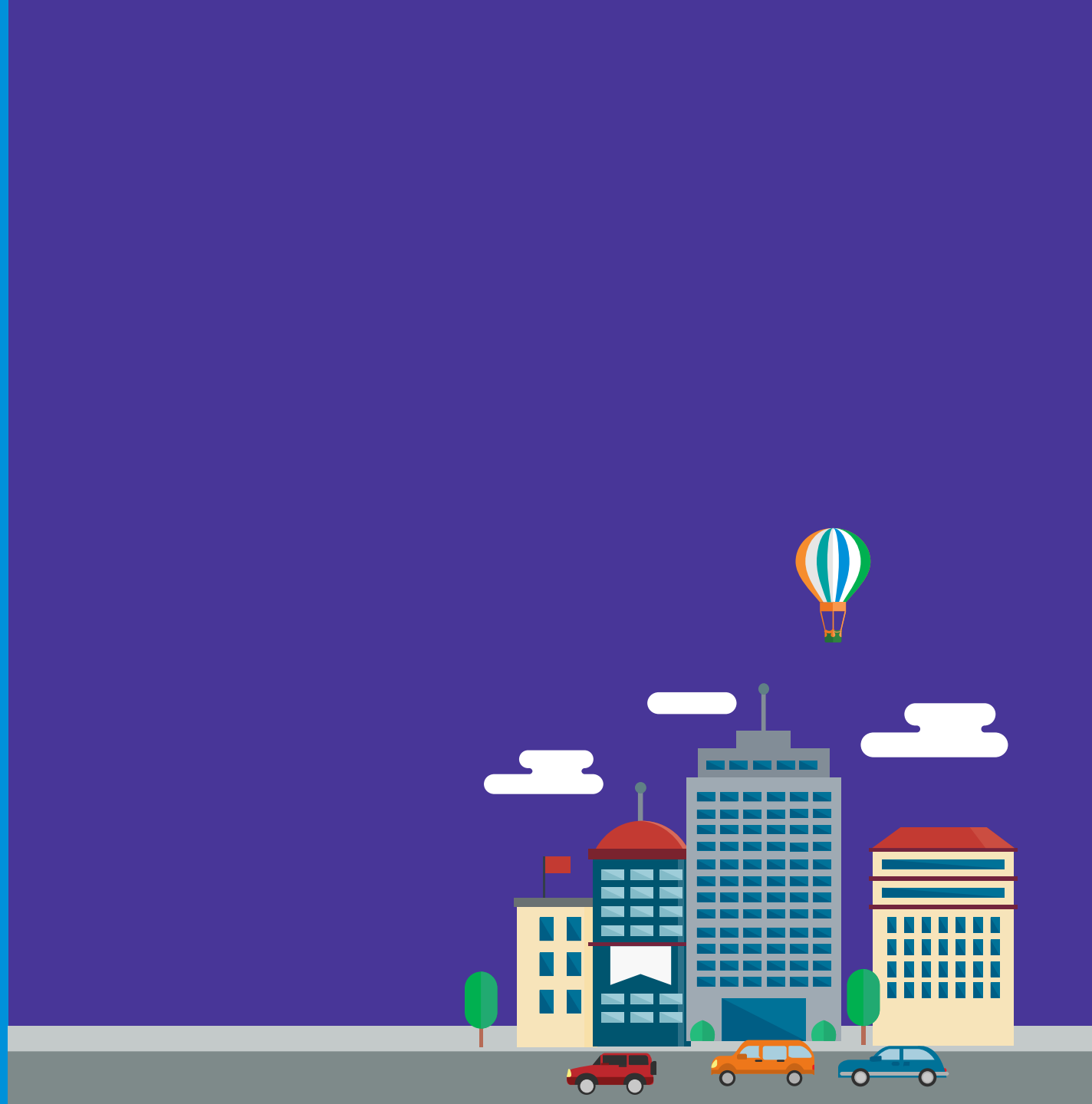
KPMG

Hacking Self-defense - essential tools for everyone

BC Security Day

May 2018



Welcome

Guy Rosario
Manager, KPMG
Office: 778 587 7888
grosario@kpmg.ca

- Over 20 years Cybersecurity experience
  - Penetration Testing, Vulnerability Assessments, security architecture reviews, Security Awareness Training
- Vice-President, ISACA Victoria Chapter
- Why I love my job

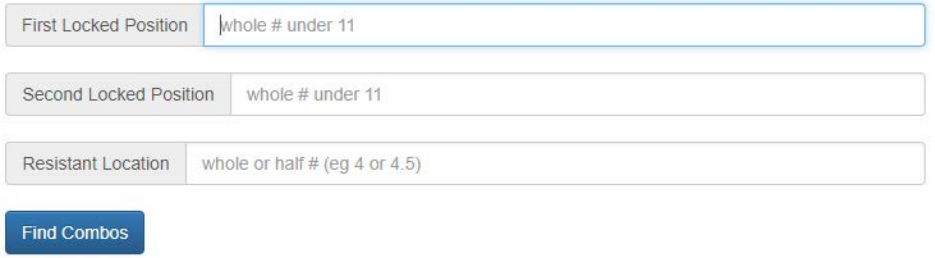
Agenda

- What’s old is new
- Find it
- Fix it
- Run it

What's old, is new…

Physical Attacks

- Oldest tricks in the book
- Can be done anytime
- Can be automated
- Often overlooked
- Low-tech still works (Cables N'Cards)
- Alarms on doors, anyone?



What's old, is new…

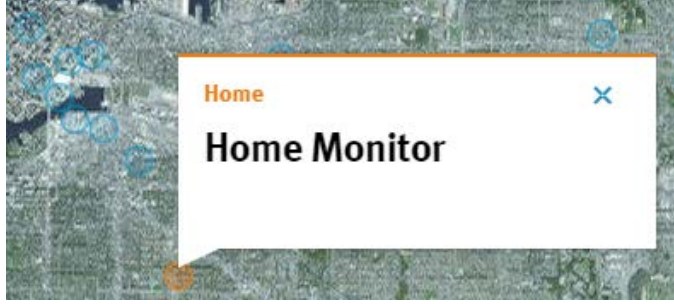
Physical Defenses

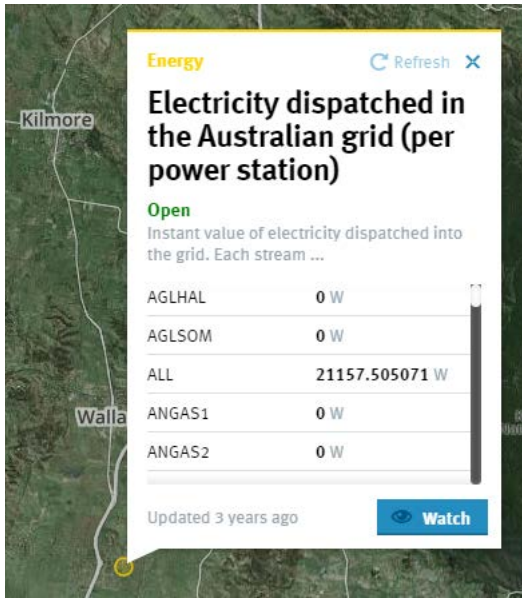
- Know what makes your physical security look easy
  - Doors need love
  - Plates, bars and posts
- Know what makes people look vulnerable
  - Kill 'em with kindness
  - Do ask and do tell

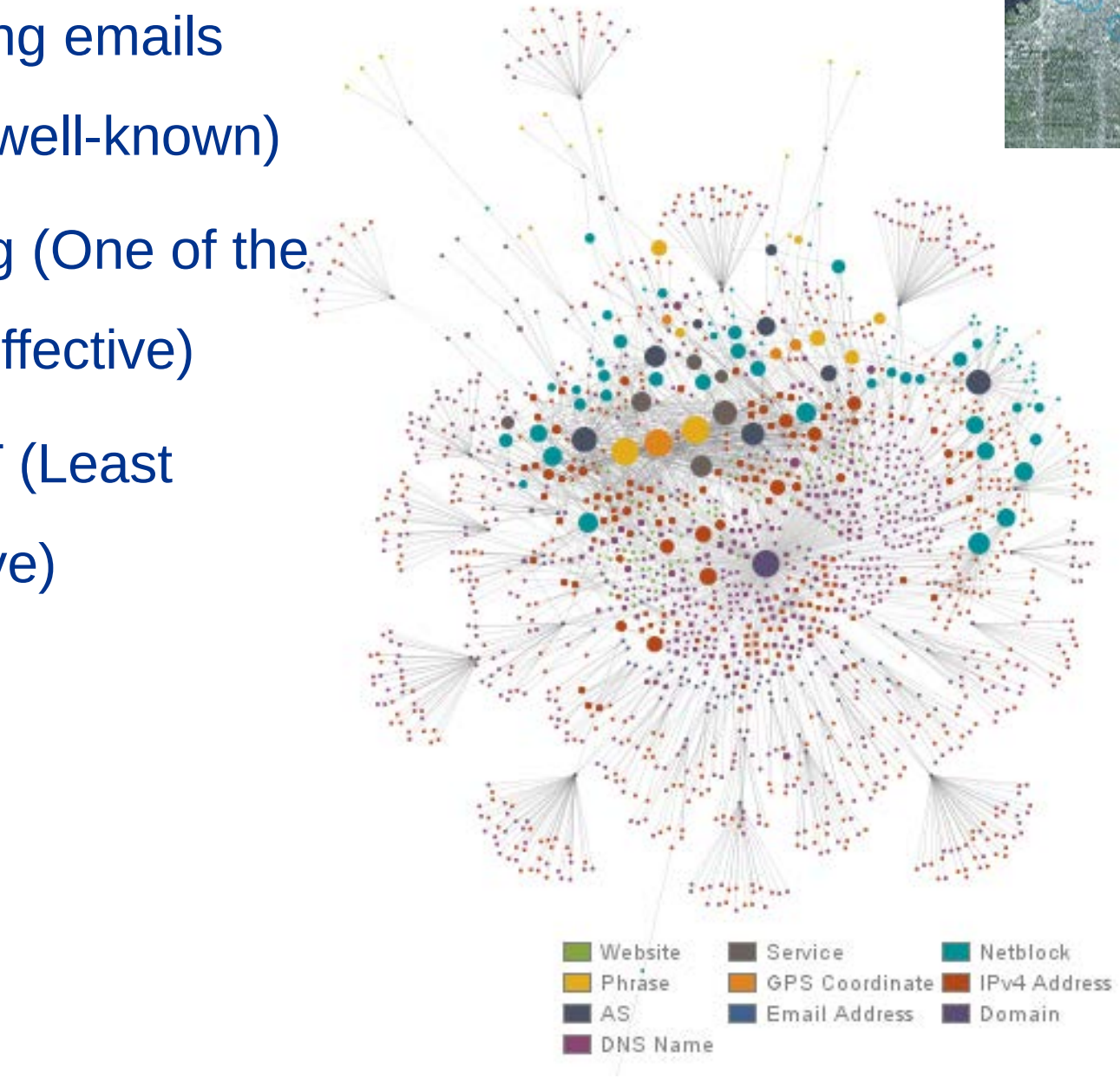
What's old, is new…

Social Attacks

- Phishing emails (most well-known)
- Vishing (One of the most effective)
- OSINT (Least Invasive)







What’s old, is new…

Social Defense

- "What's your extension and email?"
- Know what's out there.

What's old, is new…

Network Attacks

- Old 10 year old network attacks (Layer 2/3)
- WPAD
- AD hidden objects
- SNMP
- NetBIOS
- Password cracking is WAYYY faster today

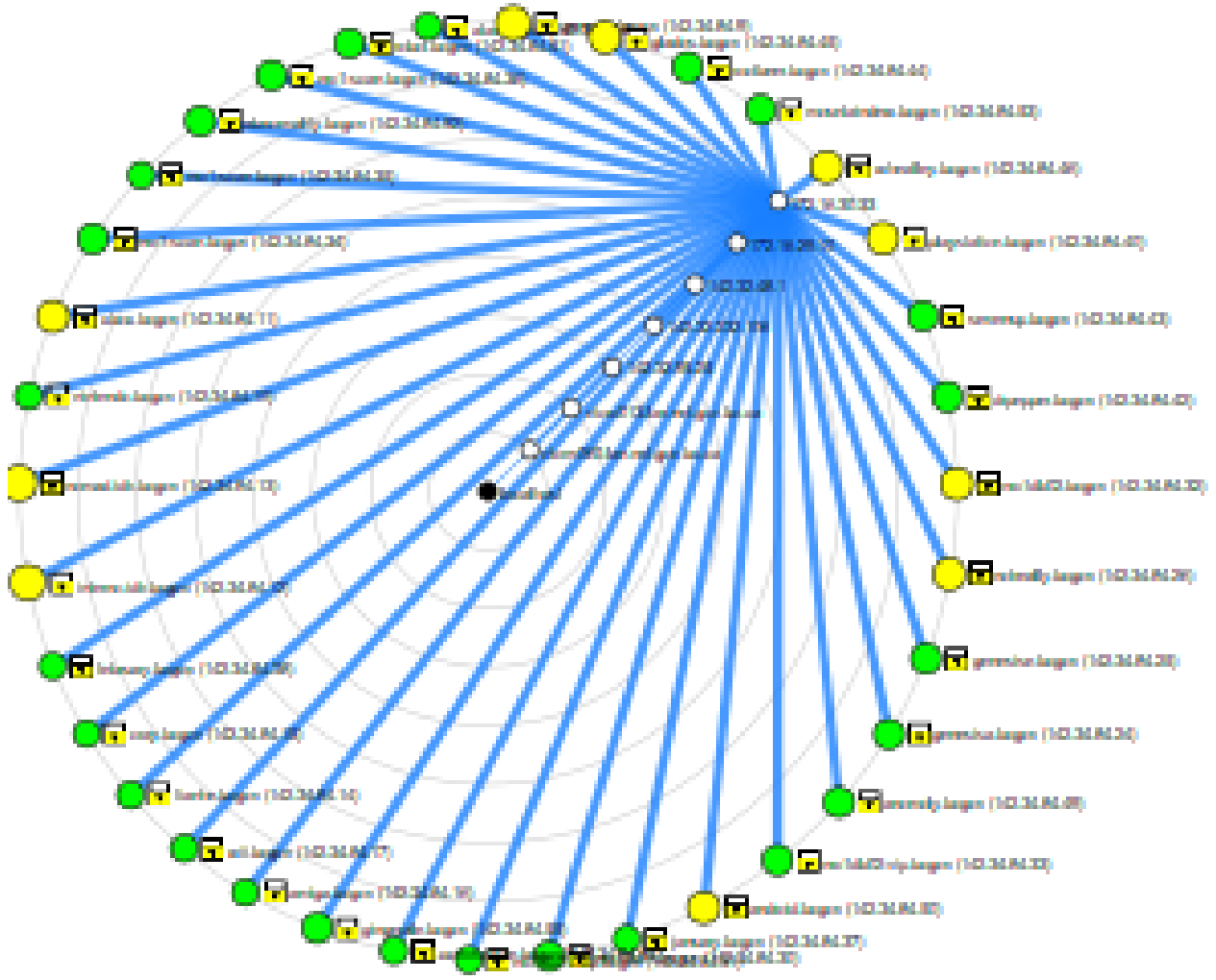
What's old, is new…

Network Defense

- L2/L3: Security is often "baked in" - Turn it on
  - (Example Cisco guidance)
  - https://www.cisco.com/c/dam/global/en_ae/assets/exposaudi2009/assets/docs/layer2-attacks-and-mitigation-t.pdf
- Know what's on your network (Asset Management)
- Find vulnerabilities BEFORE the bad guys do
- Gain visibility of a real-world attack (Ransomware example

Find it…

- Get visibility (Mac/Windows/*NIX)
  - Open Source
  - Low Cost
  - Simple to use

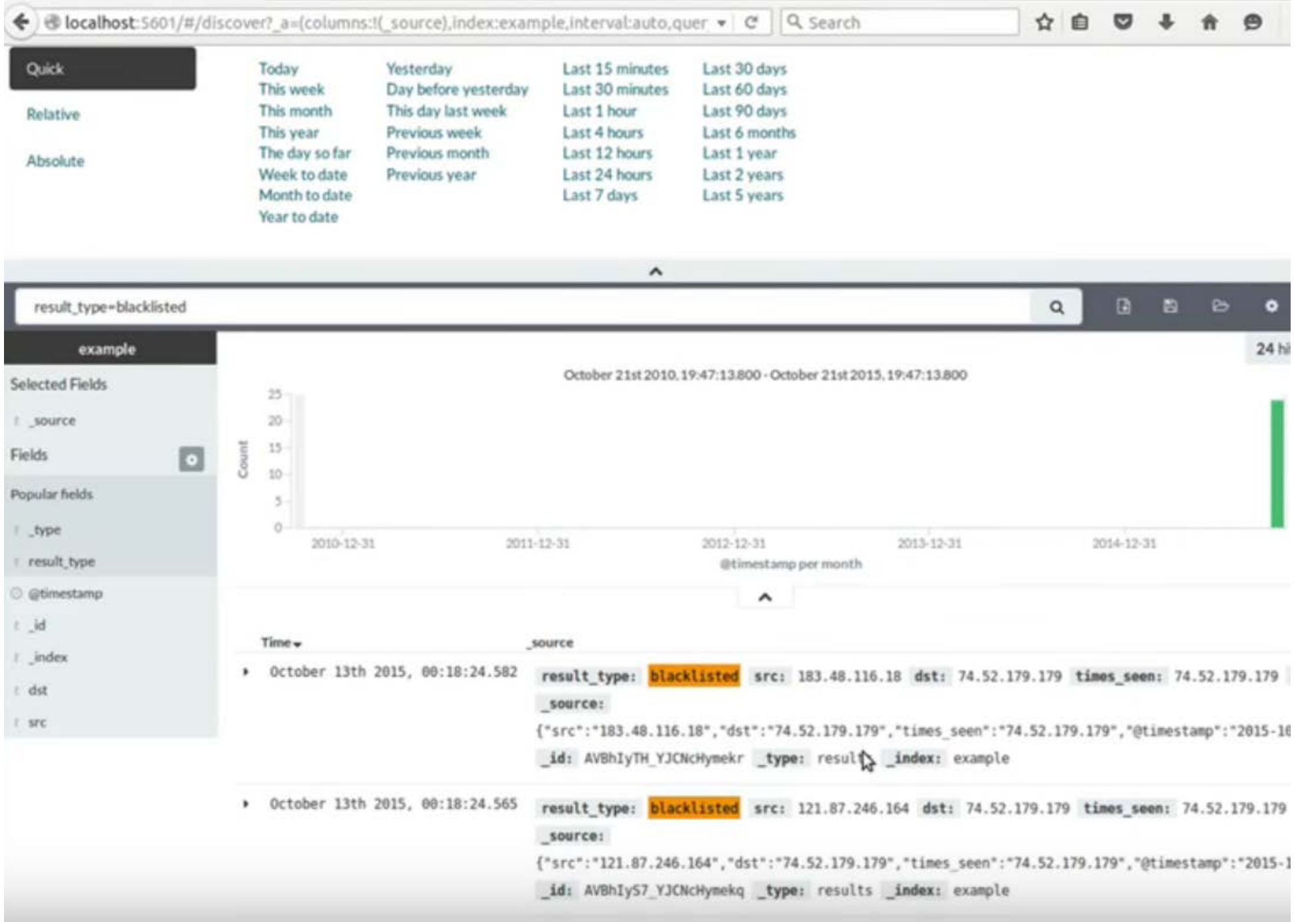


Find it…

- Know the lay of the land
  - How many systems do you have?
  - What are their names and IP addresses?
  - What version of OS and software do they have?
  - What is happening on your network?

Find it…

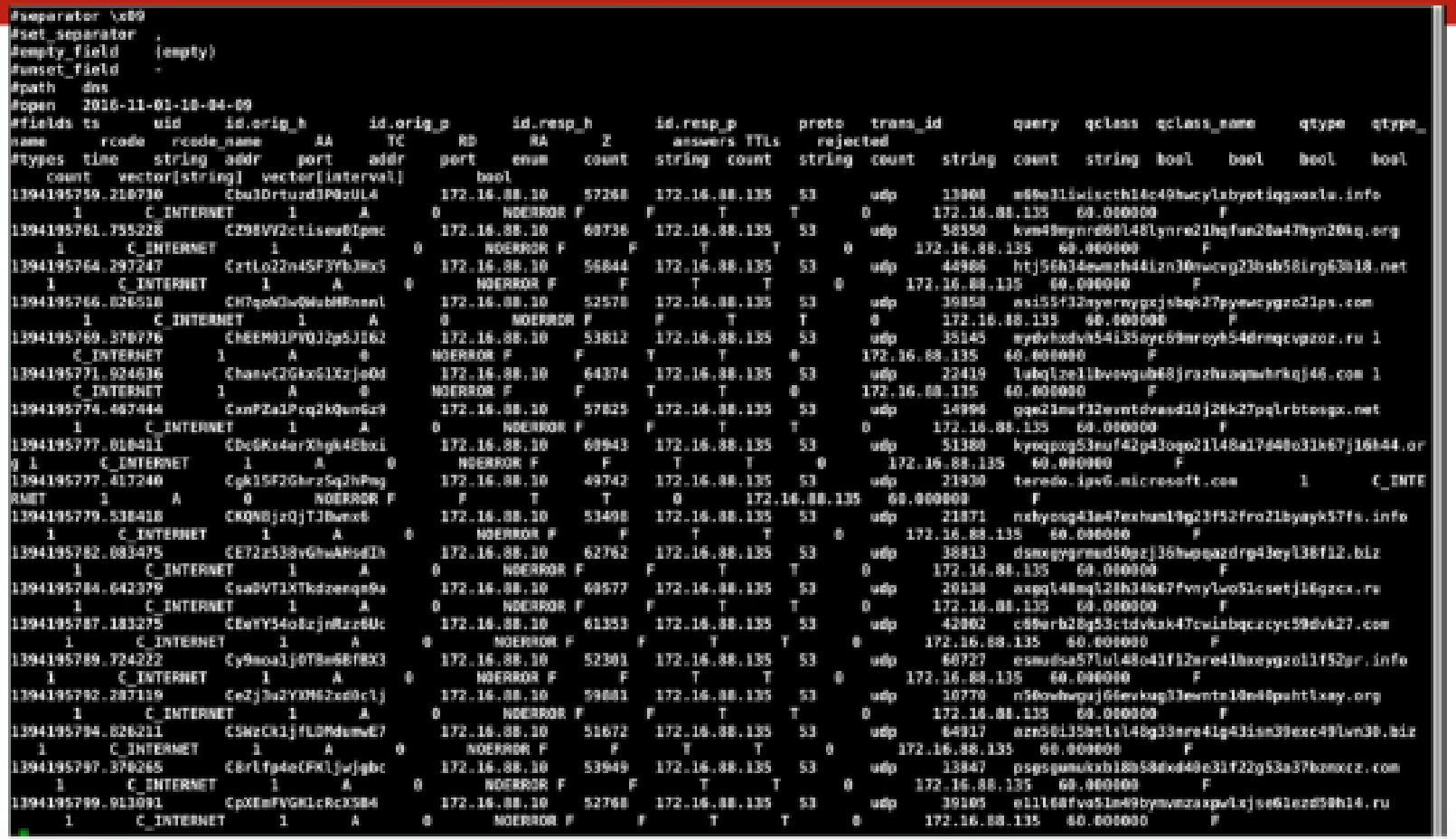
Example: Blacklisting



Some Important Logs: DNS

Find it…

Example: DNS

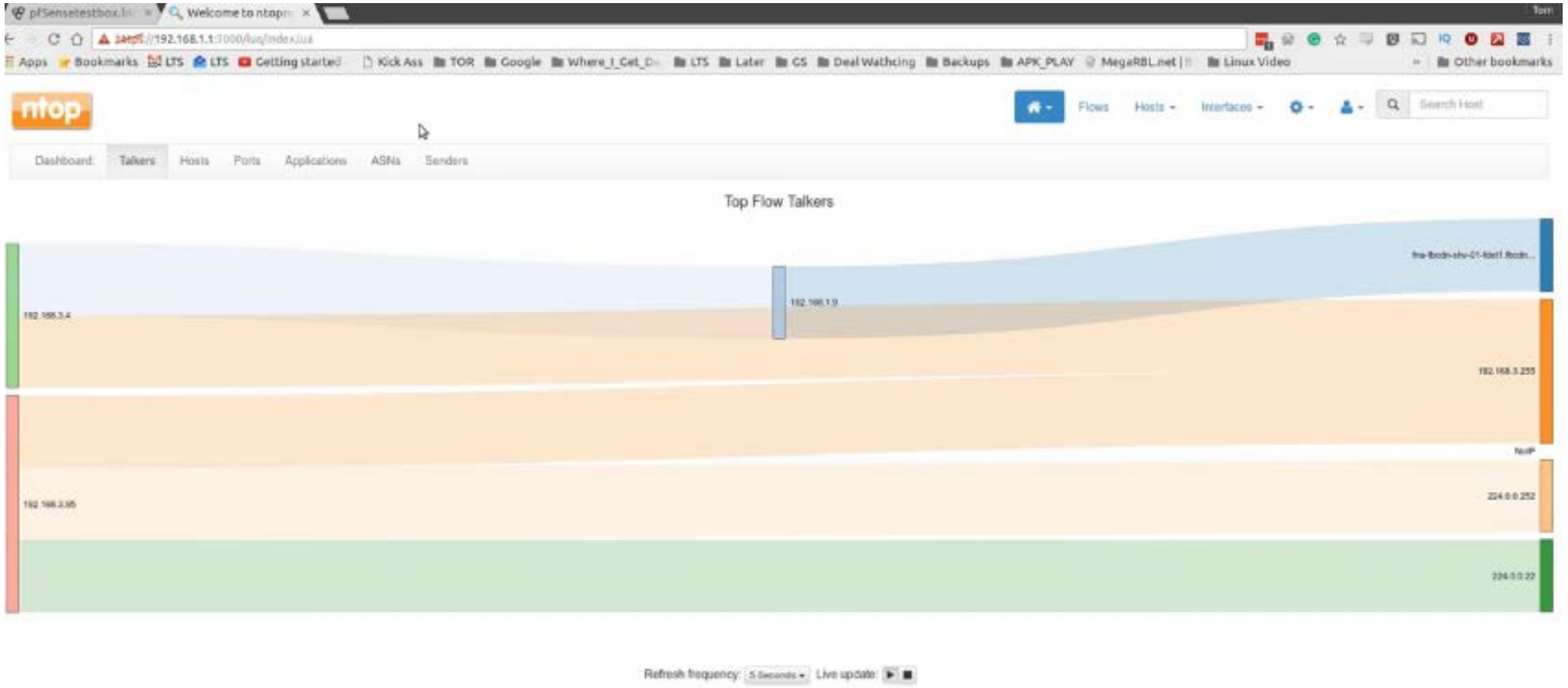


```
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   dns
#open   2016-11-01-18-04-09
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   trans_id        query   qclass  qclass_name     qtype   qtype_
name    rcode   rcode_name      AA      TC      RD      RA      Z       answers TTLs    rejected
#types  time    string  addr    port    addr    port    enum    count   string  count   string  count   string  count   string  bool    bool    bool    bool
    count   vector[string]  vector[interval]        bool
1394195759.218730       CbuJDrtuzdJP0zUL4       172.16.88.10    57268   172.16.88.135   53      udp     13008   m69a11iwiscth14c49hucylxbyotiqgxaxla.info
    1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195761.755228       CZ98VV2ctiseu0Ipmc      172.16.88.10    60736   172.16.88.135   53      udp     58550   kwn48mynrd60l48lynre21hqfun2ba47hyn20kq.org
    1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195764.297247       CztLo22n4SF3YbJRc5      172.16.88.10    56844   172.16.88.135   53      udp     44986   htj56h14ewmzh44izn30nwcwg23bsb58irg63b18.net
    1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195766.026518       CH7qoW3wQWubMRnnnl      172.16.88.10    52578   172.16.88.135   53      udp     39858   asi55f32myernygzxjsbqk27pyewcygzc21ps.com
    1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195769.370776       ChEEM01PVQJ2g5JI62      172.16.88.10    53812   172.16.88.135   53      udp     35145   mydvhzdvk54i35ayc69mrcyh54drmqcvgzoz.ru 1
    C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195771.924636       ChanvC2GkxGlXzjo0d      172.16.88.10    64374   172.16.88.135   53      udp     22419   labqlze11bvsvgub68jrazhaaqmwhrkqj46.com 1
    C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195774.467444       CxnPZa1Pcq2kQun6z9      172.16.88.10    57825   172.16.88.135   53      udp     14996   gqe21muf32evntdvasd10j26k27pqlrbtosgx.net
    1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195777.018411       CDcGKx4arXhgk4Ebxi      172.16.88.10    60943   172.16.88.135   53      udp     51380   kyoqpog53euf42g43oqe21l48a17d48o31k67j16b44.or
g 1     C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195777.417240       Cgk15F2GbrzSq2hPmg      172.16.88.10    49742   172.16.88.135   53      udp     21930   teredo.ipv6.microsoft.com       1       C_INTE
RNET    1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195779.538418       CKQN0jzQjTJBwnx6        172.16.88.10    53498   172.16.88.135   53      udp     21871   nxhyoug43m47mxhum19g23f52fro21byayk57fs.info
    1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195782.083475       CE72z538vGhwAHsdIh      172.16.88.10    62762   172.16.88.135   53      udp     38813   dsmxgygrmsd50grj36hwpqazdrg43eyl38f12.biz
    1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195784.642379       Csa0VT1XTkdzenqn9a      172.16.88.10    60577   172.16.88.135   53      udp     20138   axqql48mq128h34k67fvnylwo51csetj16gzcx.ru
    1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195787.183275       CEaYY54o8zjnMzz8Uc      172.16.88.10    61353   172.16.88.135   53      udp     42002   c89erb28g53ctdvkxk47cwixbqczcyc59dvk27.com
    1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195789.724222       Cy9noalj0T8n6BfBX3      172.16.88.10    52301   172.16.88.135   53      udp     60727   esmu0sa57lul48o41f12ere41bxeygzo11f52gr.info
    1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195792.287119       CeZj3u2YXM62xd0clj      172.16.88.10    59881   172.16.88.135   53      udp     10770   n50owhwgqzj66evkug33ewnts10m40pshtlxay.org
    1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195794.026211       C5WzCk1jfLDMdumwE7      172.16.88.10    51672   172.16.88.135   53      udp     64917   azn50i35btli140g33nre41g43isn39exc49lwn30.biz
    1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195797.370265       C8rlfg4eCPKljwjgbc      172.16.88.10    53949   172.16.88.135   53      udp     13847   psgsgumuXxbl80b58d0d40e31f22g53a37bxmxzz.com
    1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
1394195799.913091       CpXEmFVGKlcRcX5B4       172.16.88.10    52768   172.16.88.135   53      udp     39105   gll168fva51m49bymvmzaxpwlxjse61ezd58h14.ru
    1       C_INTERNET      1       A       0       NOERROR F       F       T       T       0       172.16.88.135   60.000000       F
```

https://bitbucket.org/ethanr/dns-blacklists/

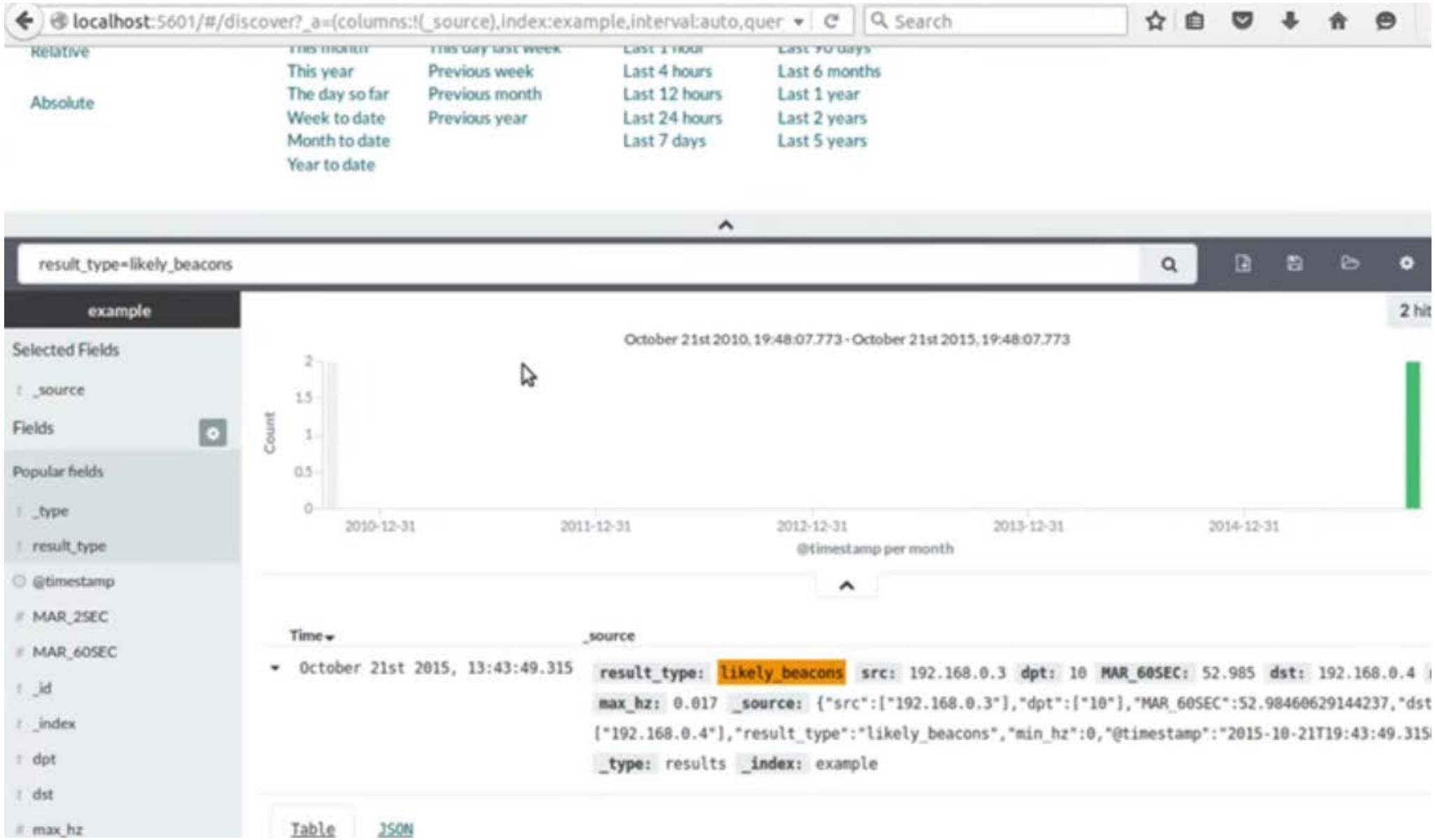
Find it…

Example: Network Flow



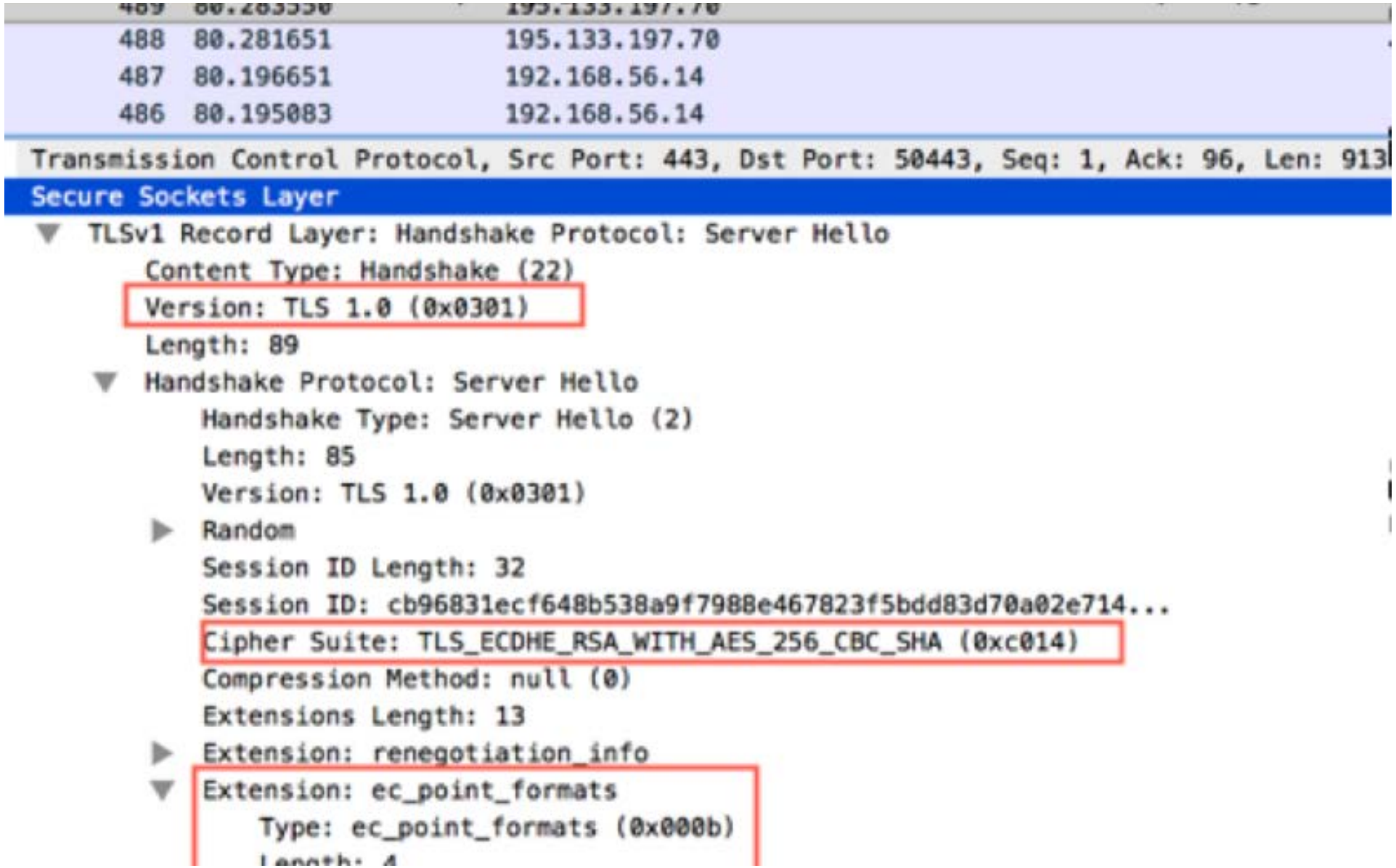
Find it…

Example: Beacons



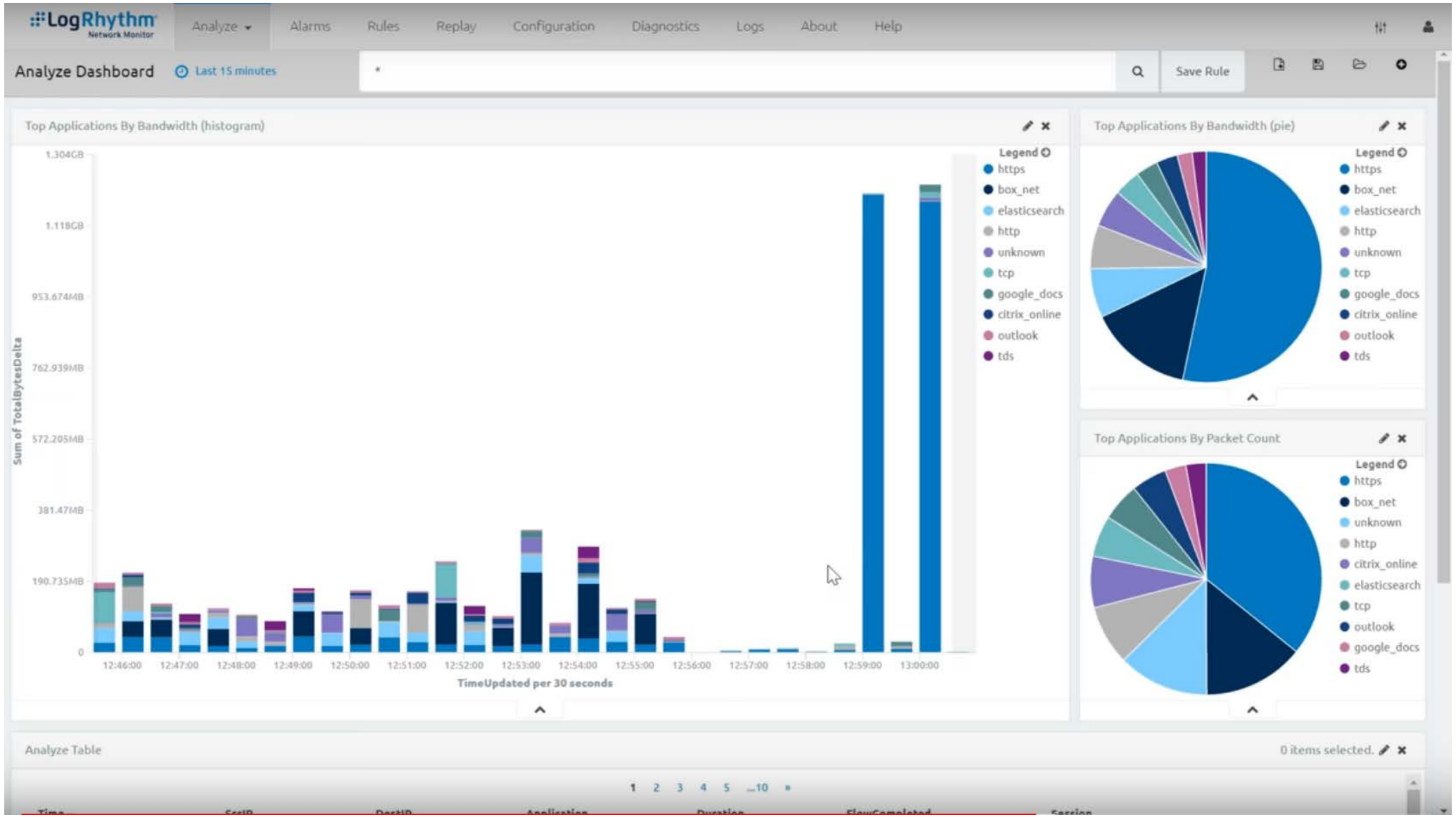
Find it…

Example: TLS Sigs & Beacons



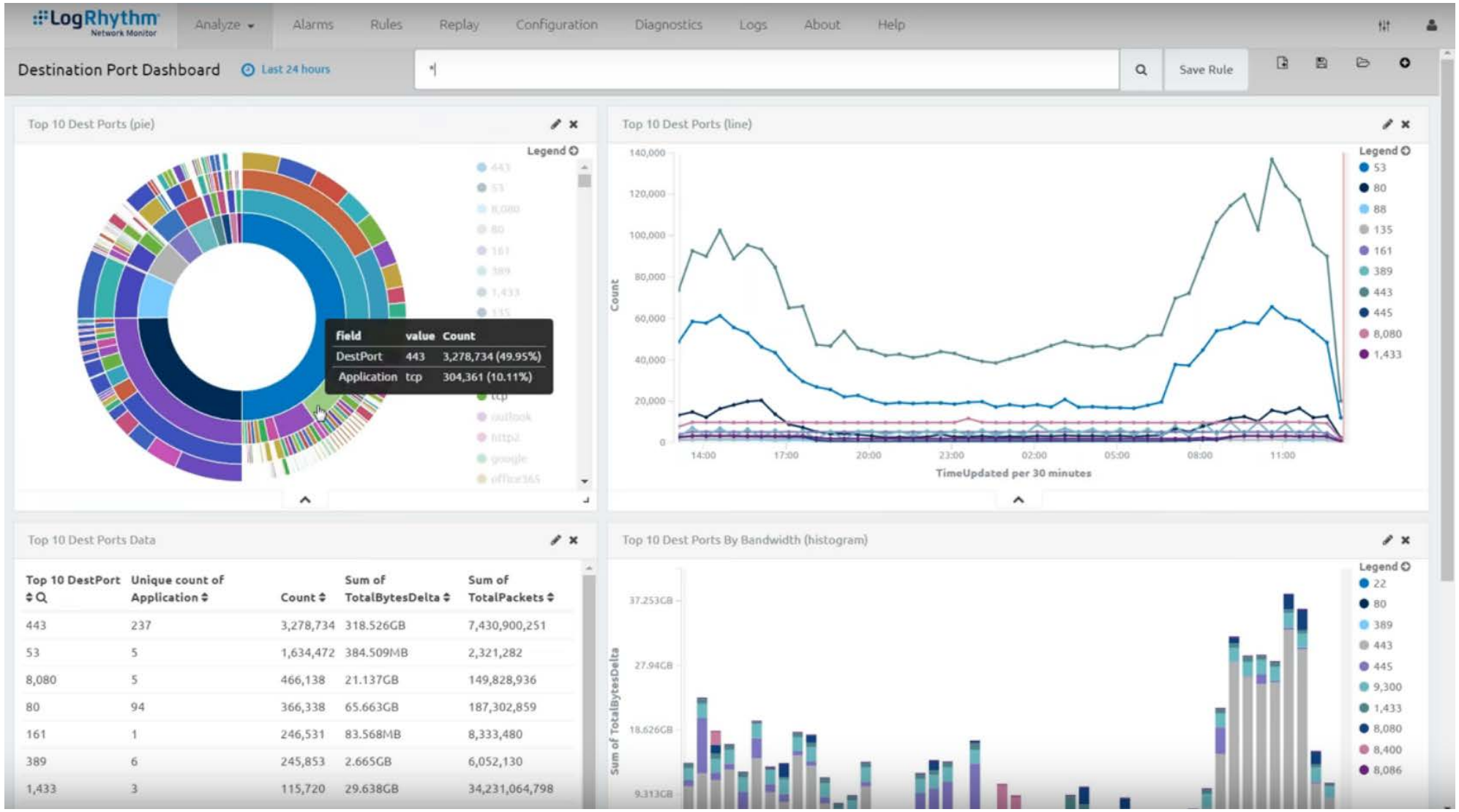
Find it…

Example: Visibility



Find it…

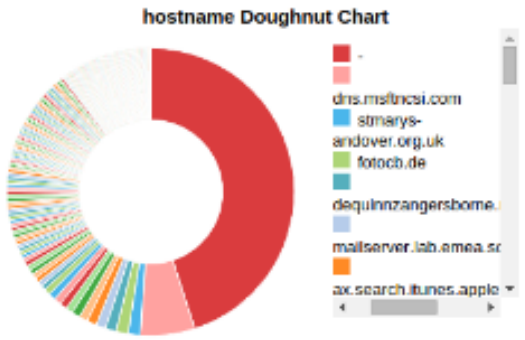
Example: Visibility



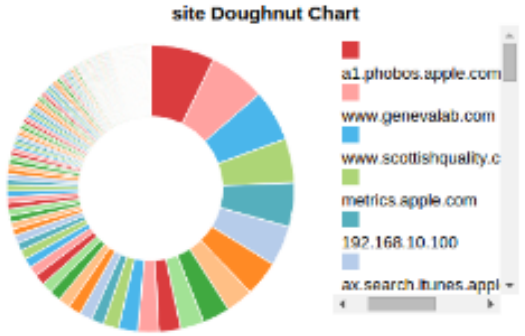
Find it…

Example: Visibility

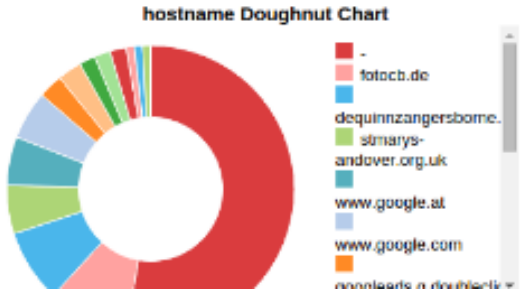
Hostnames - DNS, HTTP, SSL



hostname	class=BRO_DNS dstport="53" groupby:hostname
-	331
dns.msftncsi.com	45
fotocb.de	10
stmarys-andover.org.uk	10
dequinnzangersborne.nl	9
ax.search.itunes.apple.com	8
mailserver.lab.emea.sourcefire.com	8
www.google.com	7
google.com	7
ax.itunes.apple.com	6
time.windows.com	6



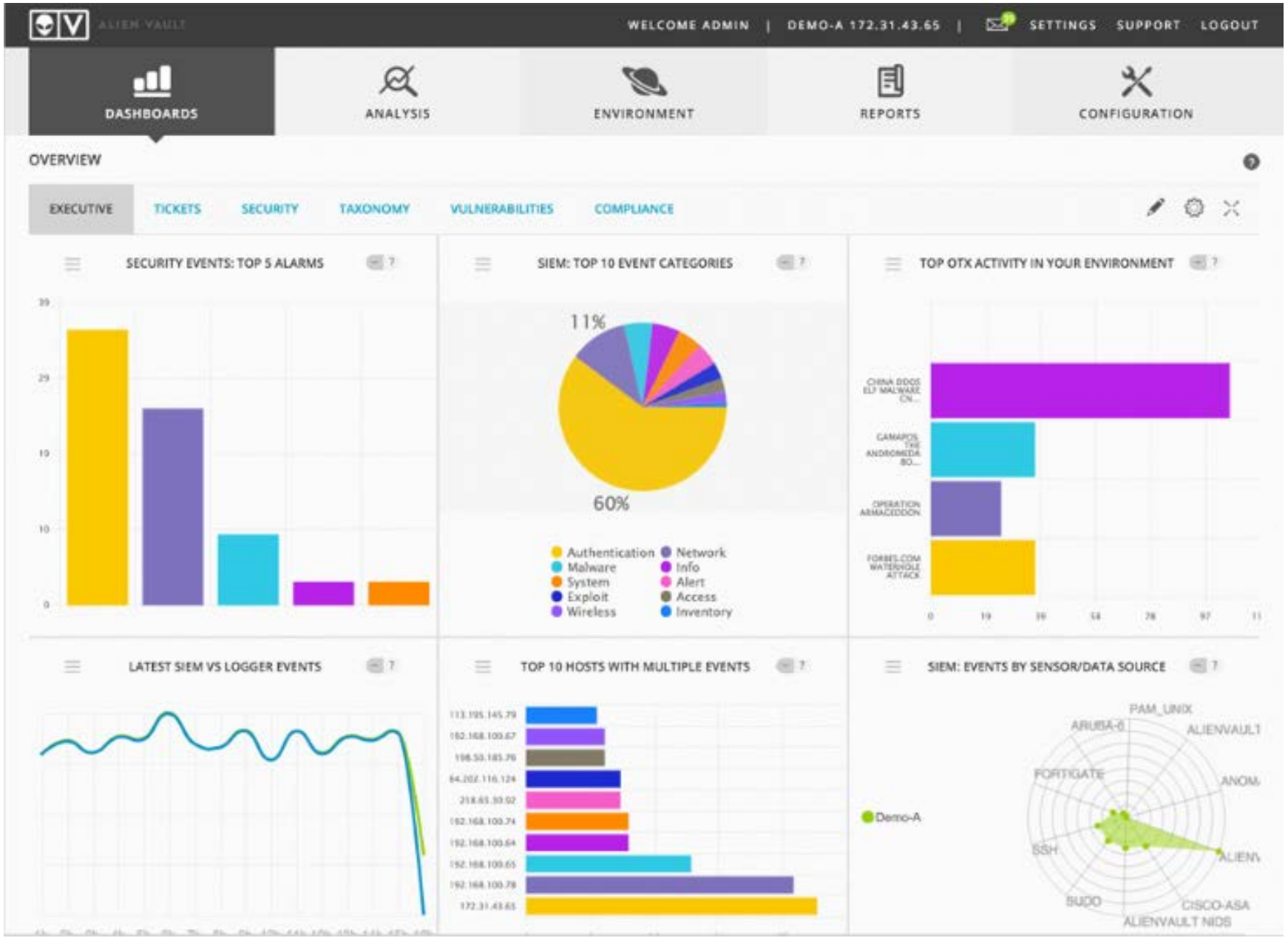
site	class=BRO_HTTP "-" groupby:site
a1.phobos.apple.com	96
www.genevalab.com	85
www.scottishquality.com	77
192.168.10.100	66
metrics.apple.com	66
ax.search.itunes.apple.com	60
www.excelforum.com	53
-	41
pagead2.googlesyndication.com	41
www.theopen.be	35
s.newsnow.net	33



hostname	class=BRO_SSL "-" groupby:hostname
-	58
fotocb.de	10
dequinnzangersborne.nl	9
stmarys-andover.org.uk	6
www.google.at	6
www.google.com	6
googleads.g.doubleclick.net	3
fbstatic-a.akamaihd.net	3
aemmiphbweeuef59.com	2
www.gstatic.com	2

Find it…

Example: Visibility



Find it…

Example: Hidden AD Objects

- AD Object Detector tool
- Microsoft's Guidance on Hidden Folders etc…
  - https://technet.microsoft.com/en-us/library/gg456494.aspx
- CrowdStrike - Bloodhound

Hidden Administrative Accounts: BloodHound to the Rescue

April 24, 2018 Vincent Uguccioni From The Front Lines

Fix it…

- These will give free advice on fixing things:
  - OpenVAS
  - Nessus (Community Version)
  - Microsoft
  - NIST
  - OWASP Zap

Run it…

- I can only show you the path… you have to run it…
- Start with Security Awareness training (People)
- “Start slow and go…”
- VMs are easy and safe way to begin…
  - Armitage
  - Bro
  - LogRhythm
  - pfSense
  - RITA
  - Security Onion
  - SELKS
  - Etc.
- Eventually, dedicated resources (People, Technology)

Demo and/or Questions

Questions?