WLCG SOC Motivation

Shawn McKee / University of Michigan

PATh PARTNERSHIP to ADVANCE THROUGHPUT COMPUTING

OSG

HTC CENTER FOR HIGH THROUGHPUT COMPUTING

Why WLCG SOC?

AGLT2 has been concerned about operational security for a lon

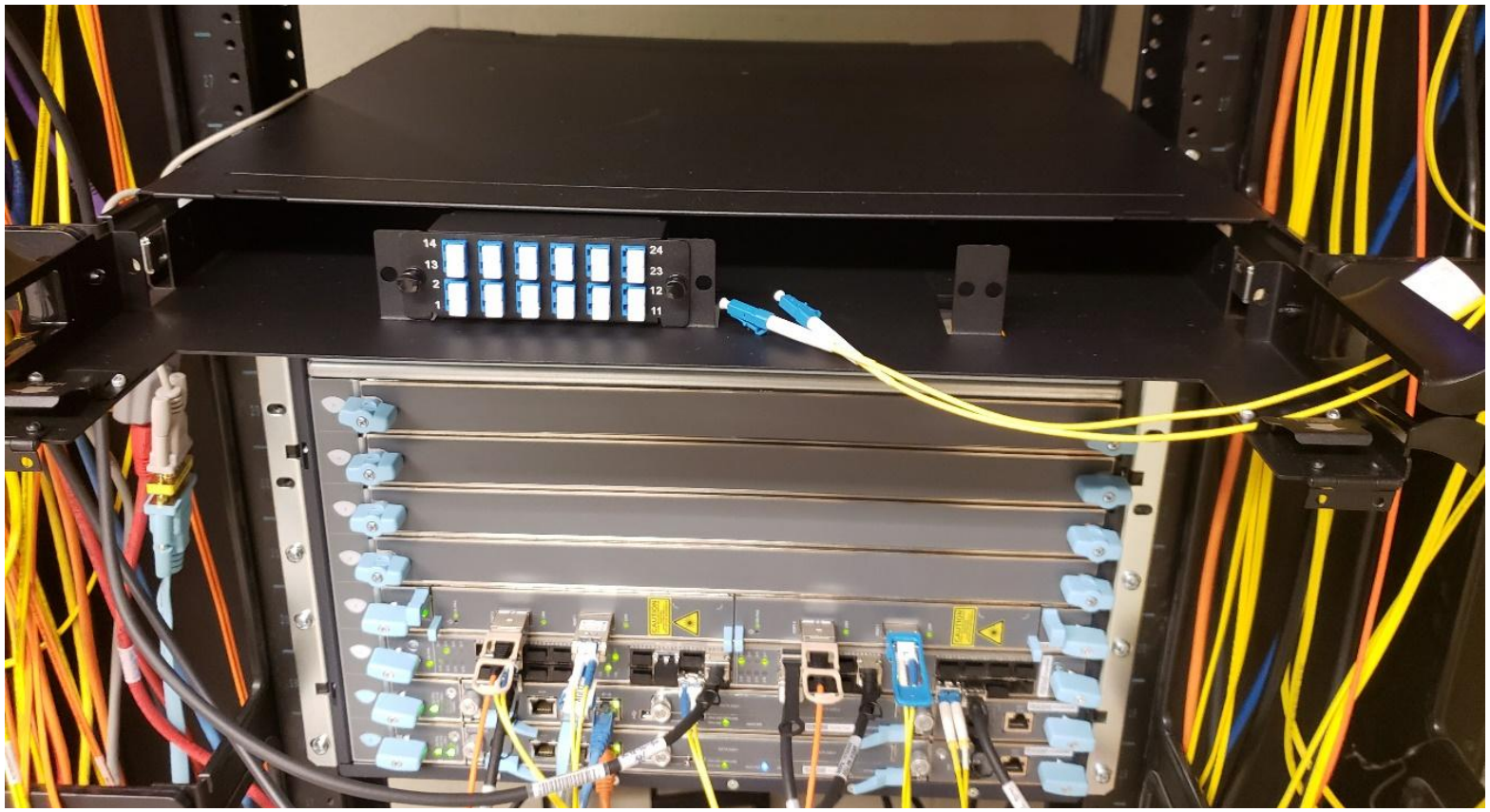
- Limited manpower at a Tier-2 and overloaded
- Would like to benefit from the broader community actively in operational security

USATLAS has also discussed how best to implement security r distributed facilities.

WLCG Security Operations Center effort seemed like a good op

- Provides example best practices, tools and docs

Original Optical Splitter / Bro / MISP



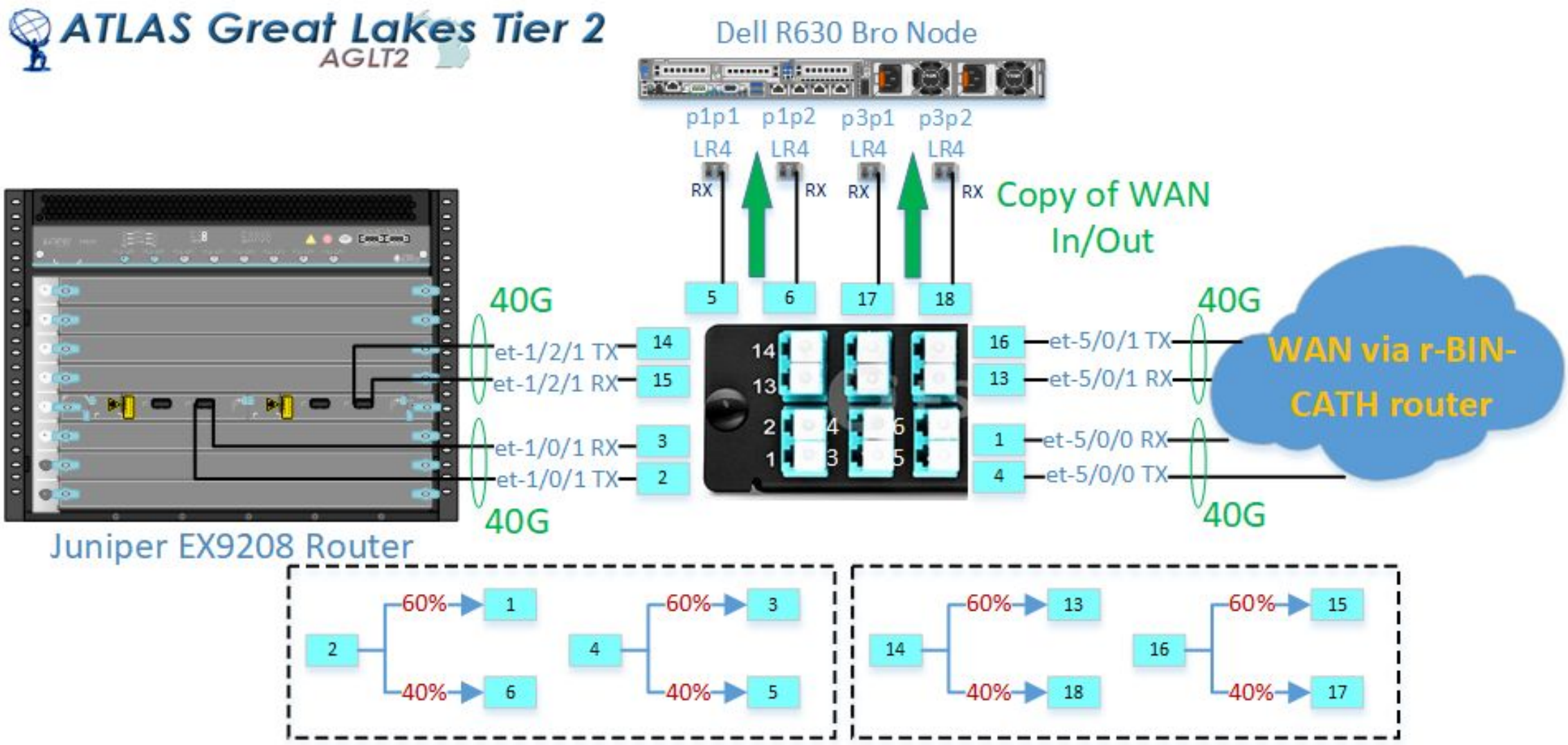
bro.aglt2.org
misp.aglt2.org

Was inexpensive to enable (~$1.2K). Splitter and shelf was $300, Intel XL710-Q2 40G nics $400 x2, $100 in cables (reused worker node for server)

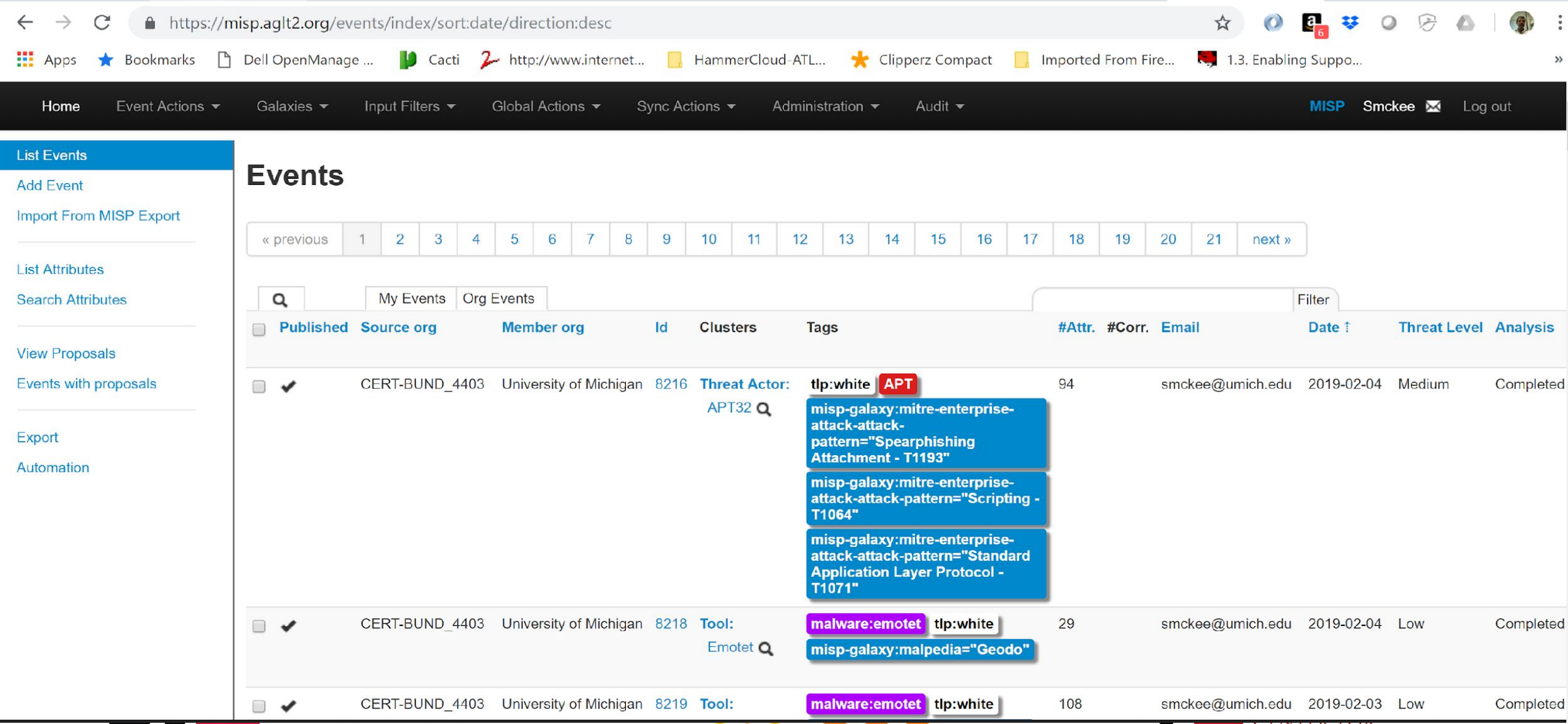
Bro (now Zeek) has been running at AGLT2 since August 10, 2018

Monthly avg of **63.1 billion** packets captured and 266 million packets lost (0.4%)

Fiber Splitter Connection Details



MISP UI

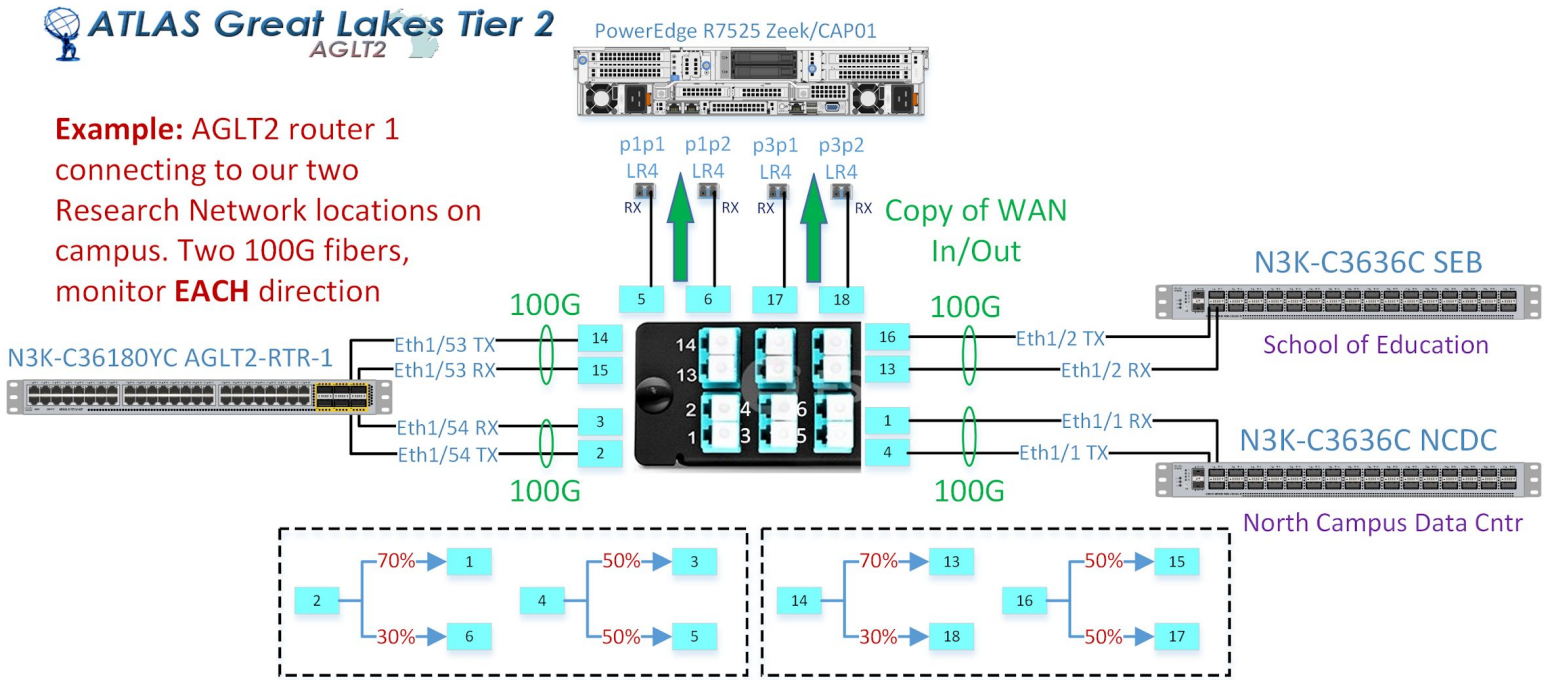

https://misp.aglt2.org/events/index/sort:date/direction:desc
Apps
Bookmarks
Dell OpenManage ...
Cacti
http://www.internet...
HammerCloud-ATL...
Clipperz Compact
Imported From Fire...
1.3. Enabling Suppo...
Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
MISP
Smckee
Log out
List Events
Add Event
Import From MISP Export
List Attributes
Search Attributes
View Proposals
Events with proposals
Export
Automation
Events
« previous
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
next »
My Events
Org Events
Filter
Published
Source org
Member org
Id
Clusters
Tags
#Attr.
#Corr.
Email
Date
Threat Level
Analysis
CERT-BUND_4403 University of Michigan 8216 Threat Actor: APT32 tlp:white APT misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing Attachment - T1193" misp-galaxy:mitre-enterprise-attack-attack-pattern="Scripting - T1064" misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" 94 smckee@umich.edu 2019-02-04 Medium Completed
CERT-BUND_4403 University of Michigan 8218 Tool: Emotet malware:emotet tlp:white misp-galaxy:malpedia="Geodo" 29 smckee@umich.edu 2019-02-04 Low Completed
CERT-BUND_4403 University of Michigan 8219 Tool: malware:emotet tlp:white 108 smckee@umich.edu 2019-02-03 Low Completed

Network Security

AGLT2 has been working with the WLCG SOC effort to help secure our networks while maintaining performance

Our original network had a Zeek+MISP+Elasticsearch setup for dual 40G. Cost to set up was about $2K plus repurposing an R630

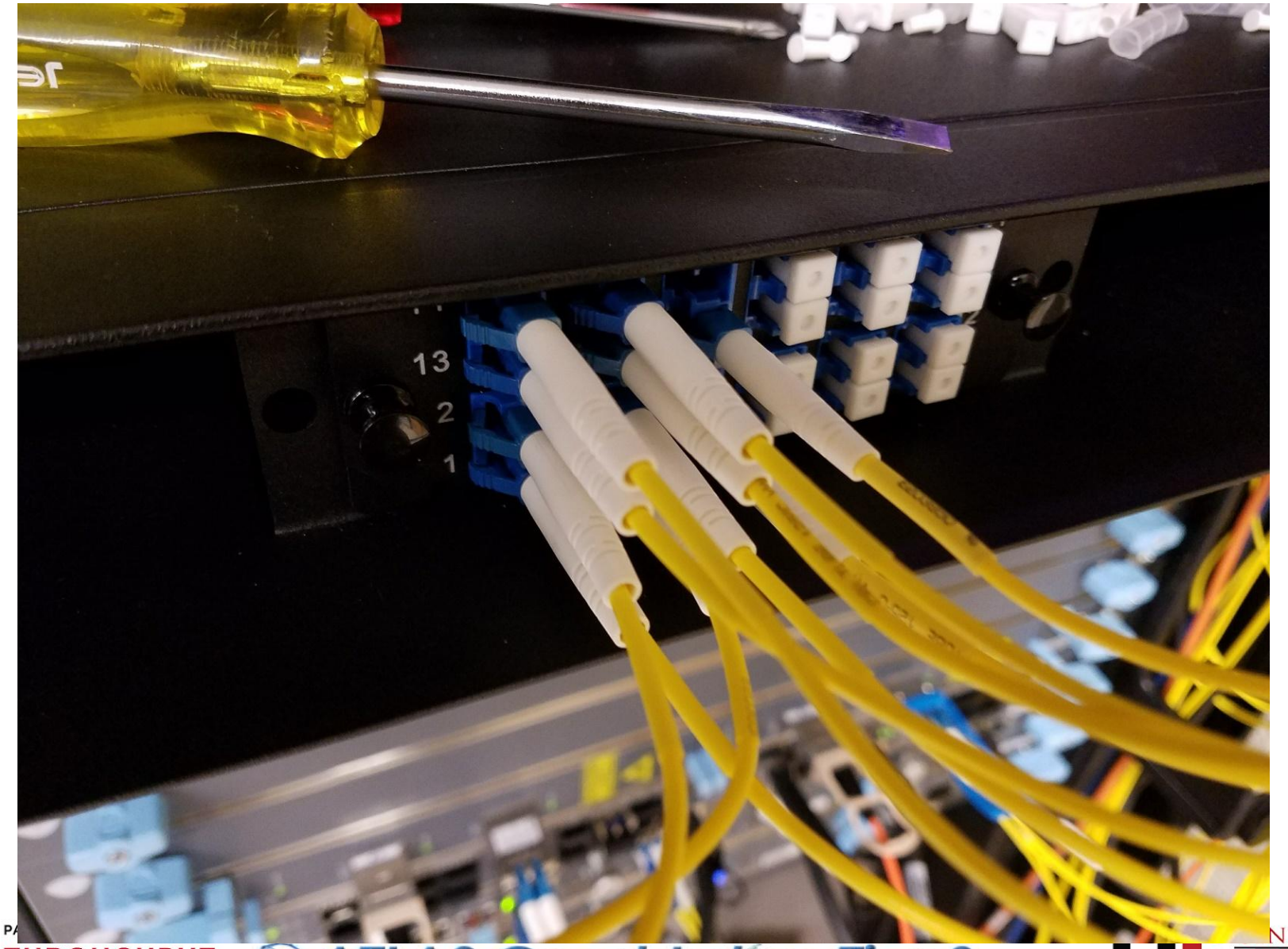
Our new network is **4x100G**
We have purchased two "network capture" nodes (Del R7525) each with two Bluefield-2 NICs (each 2x100G)
Have a milestone for July 2023 to get it into production…



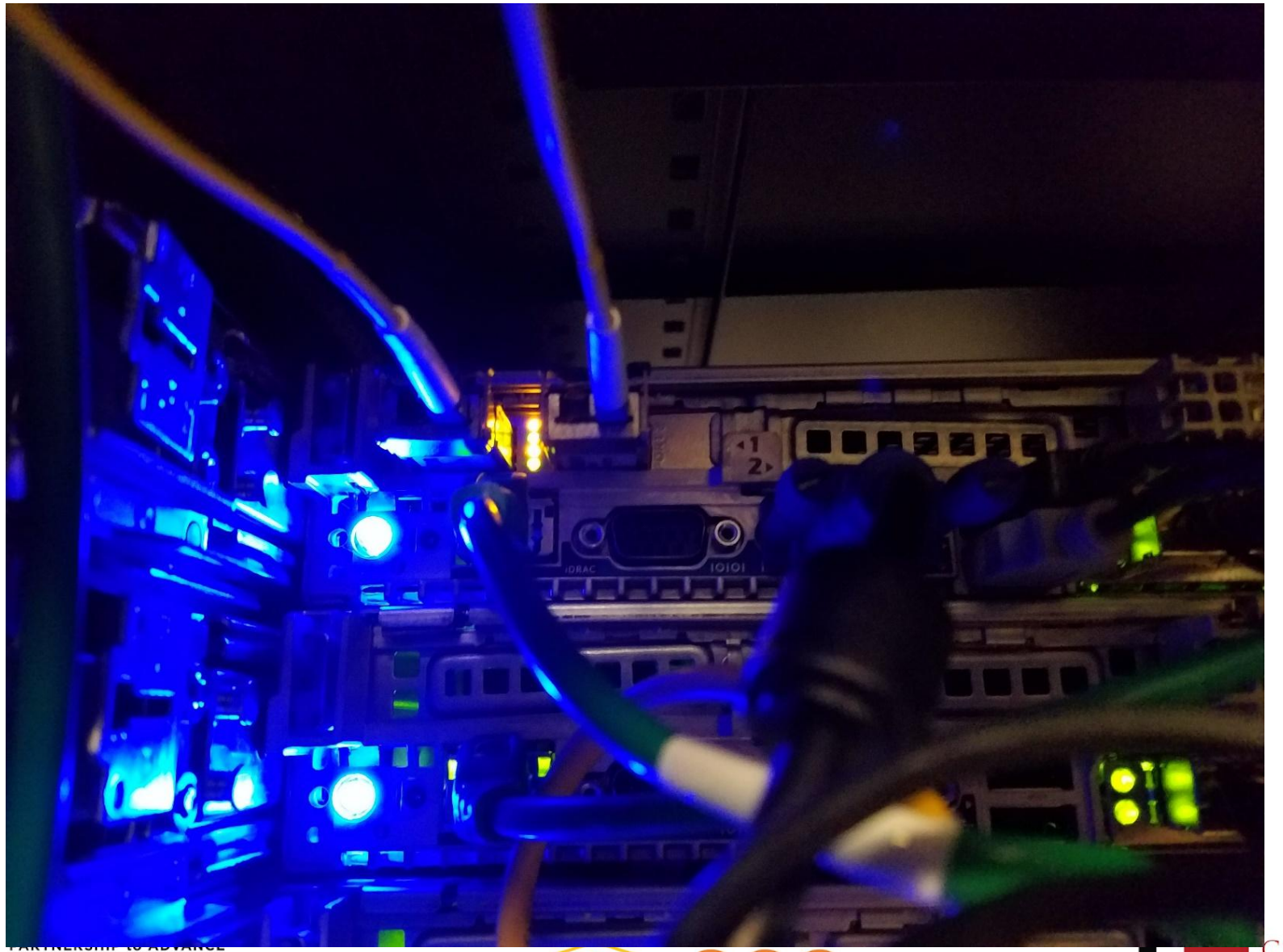
CAP01/RTR-1 diagram (similar for CAP02/RTR-2)

Additional Slides

Fiber Optical Splitter Connections



Connecton to Bro Node (1 NIC)



Bro Performance

```
[root@c-16-40 ~]# broctl capstats

Interface               kpps       mbps         (10s average)
-----------------------------------------
bro.aglt2.org/p3p1      70.5       2818.8
bro.aglt2.org/p3p2      44.1       542.5
bro.aglt2.org/p1p1      76.1       2939.8
bro.aglt2.org/p1p2      64.0       328.9

Total                   254.7      6630.0
```

```
[root@c-16-40 ~]# broctl status
Getting process status ...
Getting peer status ...
Name         Type    Host                 Status    Pid    Peers  Started
                     org                  running   3607157 25     12 Feb 09:14:24
                     org                  running   3607206 25     12 Feb 09:14:25
                     o.aglt2.org          running   3607531 2      12 Feb 09:14:27
                     o.aglt2.org          running   3607544 2      12 Feb 09:14:27
                     o.aglt2.org          running   3607557 2      12 Feb 09:14:27
                     o.aglt2.org          running   3607579 2      12 Feb 09:14:27
                     o.aglt2.org          running   3607587 2      12 Feb 09:14:27
                     o.aglt2.org          running   3607610 2      12 Feb 09:14:27
                     o.aglt2.org          running   3607605 2      12 Feb 09:14:27
                     o.aglt2.org          running   3607638 2      12 Feb 09:14:27
                     o.aglt2.org          running   3607648 2      12 Feb 09:14:27
bro.aglt2.org-p3p2-4 worker  bro.aglt2.org running   3607651 2      12 Feb 09:14:27
bro.aglt2.org-p3p2-5 worker  bro.aglt2.org running   3607690 2      12 Feb 09:14:27
bro.aglt2.org-p3p2-6 worker  bro.aglt2.org running   3607687 2      12 Feb 09:14:27
bro.aglt2.org-p1p1-1 worker  bro.aglt2.org running   3607695 2      12 Feb 09:14:27
bro.aglt2.org-p1p1-2 worker  bro.aglt2.org running   3607693 2      12 Feb 09:14:27
bro.aglt2.org-p1p1-3 worker  bro.aglt2.org running   3607698 2      12 Feb 09:14:27
bro.aglt2.org-p1p1-4 worker  bro.aglt2.org running   3607717 2      12 Feb 09:14:27
bro.aglt2.org-p1p1-5 worker  bro.aglt2.org running   3607716 2      12 Feb 09:14:27
bro.aglt2.org-p1p1-6 worker  bro.aglt2.org running   3607725 2      12 Feb 09:14:27
bro.aglt2.org-p1p2-1 worker  bro.aglt2.org running   3607741 2      12 Feb 09:14:27
bro.aglt2.org-p1p2-2 worker  bro.aglt2.org running   3607740 2      12 Feb 09:14:27
bro.aglt2.org-p1p2-3 worker  bro.aglt2.org running   3607739 2      12 Feb 09:14:27
bro.aglt2.org-p1p2-4 worker  bro.aglt2.org running   3607747 2      12 Feb 09:14:27
bro.aglt2.org-p1p2-5 worker  bro.aglt2.org running   3607748 2      12 Feb 09:14:27
bro.aglt2.org-p1p2-6 worker  bro.aglt2.org running   3607749 2      12 Feb 09:14:27
```

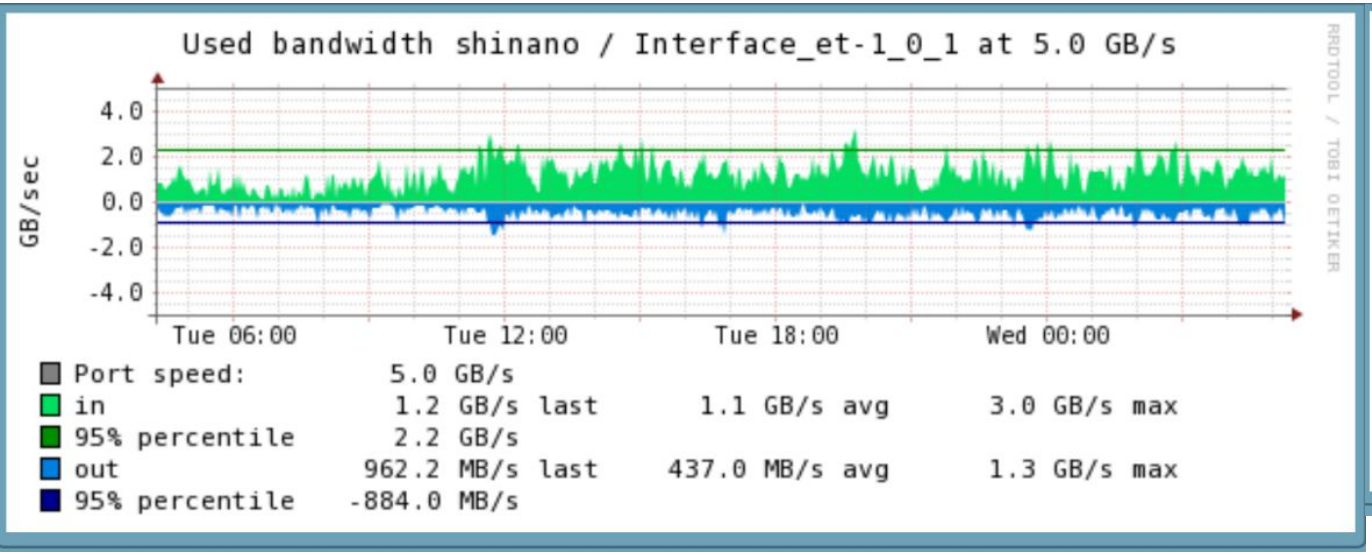
Bro Performance(2)

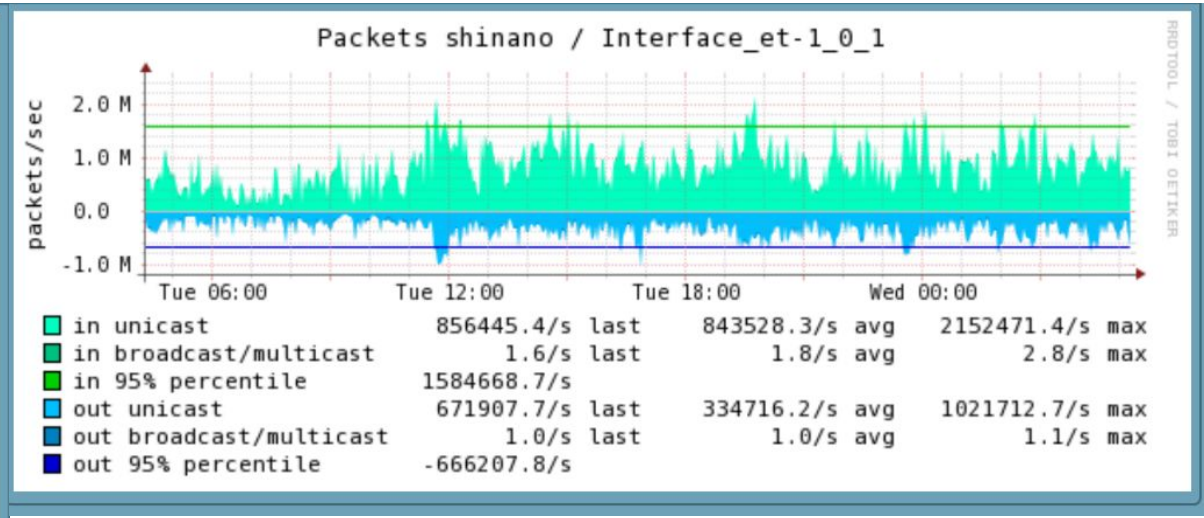
Capture of packets is reasonably efficient but highly variable

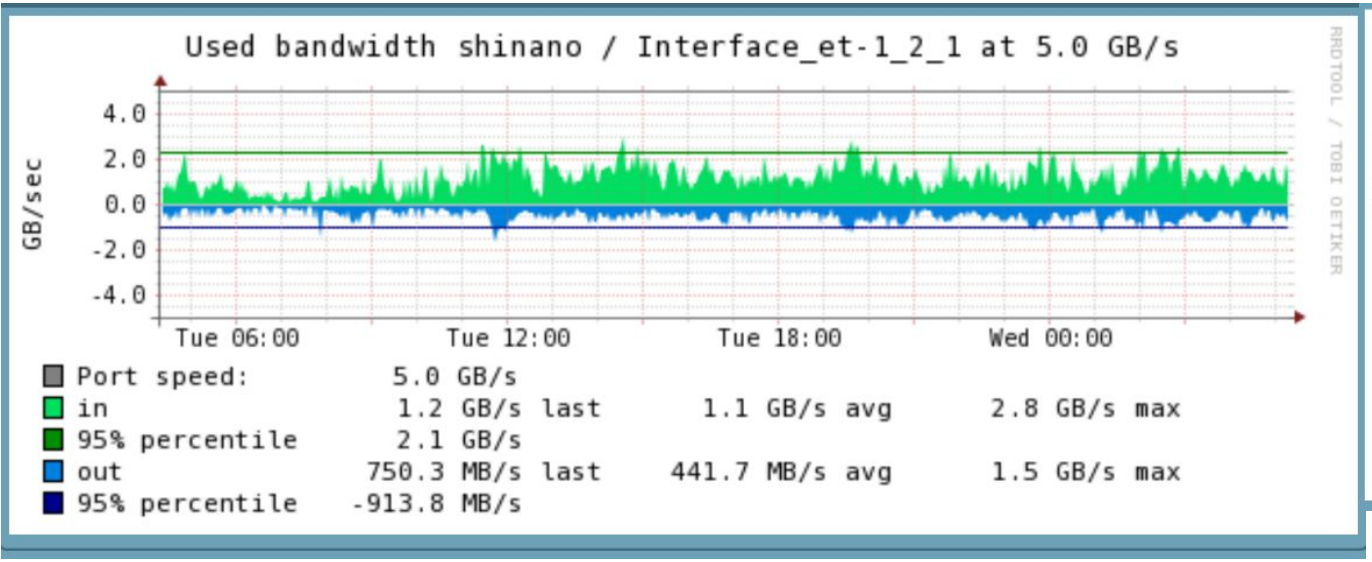
Lost packets varies from **0.1%** to **57%**, depending upon which process is involved

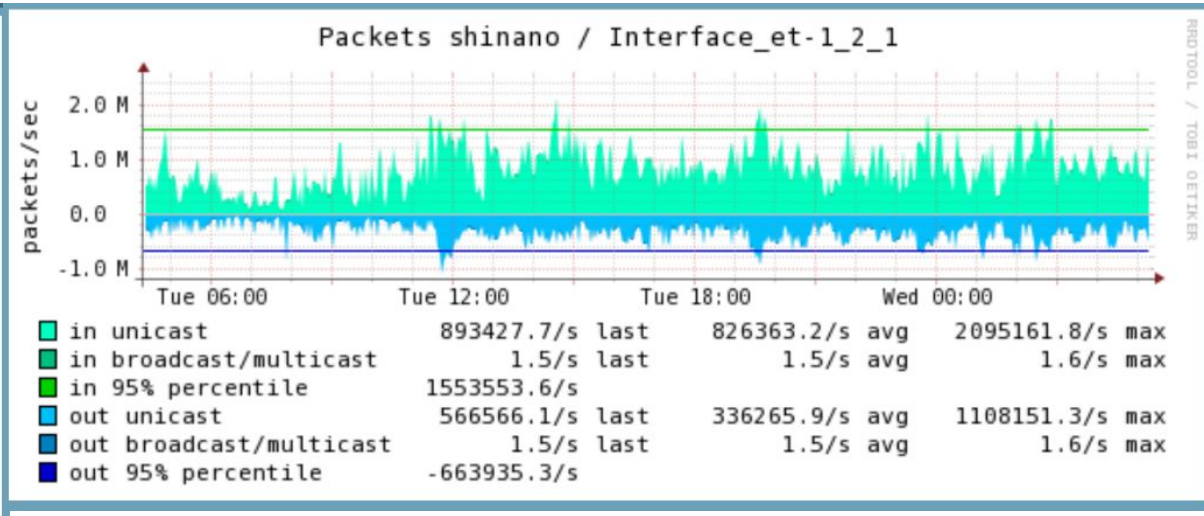
```
[root@c-16-40 ~]# broctl netstats
bro.aglt2.org-p3p1-1: 1550653692.603264 recvd=608801620 dropped=68030355 link=608801620
bro.aglt2.org-p3p1-2: 1550653692.803207 recvd=564177704 dropped=93582243 link=564177704
bro.aglt2.org-p3p1-3: 1550653693.003355 recvd=684731454 dropped=73426190 link=684731454
bro.aglt2.org-p3p1-4: 1550653693.204227 recvd=622629592 dropped=95842930 link=622629592
bro.aglt2.org-p3p1-5: 1550653693.404089 recvd=662543937 dropped=81534338 link=662543937
bro.aglt2.org-p3p1-6: 1550653693.605284 recvd=429727642 dropped=95344144 link=429727642
bro.aglt2.org-p3p2-1: 1550653693.805156 recvd=1841624176 dropped=5297094 link=1841624176
bro.aglt2.org-p3p2-2: 1550653694.006008 recvd=1575181790 dropped=6647926 link=1575181790
bro.aglt2.org-p3p2-3: 1550653694.206215 recvd=1872168909 dropped=6379723 link=1872168909
bro.aglt2.org-p3p2-4: 1550653694.406134 recvd=1672350038 dropped=5057261 link=1672350038
bro.aglt2.org-p3p2-5: 1550653694.607082 recvd=1647497318 dropped=6460379 link=1647497318
bro.aglt2.org-p3p2-6: 1550653694.807200 recvd=1630892242 dropped=7325649 link=1630892242
bro.aglt2.org-p1p1-1: 1550653695.008275 recvd=231878579 dropped=131601959 link=231878579
bro.aglt2.org-p1p1-2: 1550653695.208211 recvd=355737802 dropped=71456816 link=355737802
bro.aglt2.org-p1p1-3: 1550653695.408198 recvd=275147905 dropped=75679081 link=275147905
bro.aglt2.org-p1p1-4: 1550653695.610199 recvd=198015511 dropped=65764347 link=198015511
bro.aglt2.org-p1p1-5: 1550653695.810081 recvd=156858519 dropped=63783349 link=156858519
bro.aglt2.org-p1p1-6: 1550653696.011028 recvd=283369148 dropped=66690807 link=283369148
bro.aglt2.org-p1p2-1: 1550653696.211150 recvd=1859463556 dropped=3611770 link=1859463556
bro.aglt2.org-p1p2-2: 1550653696.411283 recvd=1676880947 dropped=2449344 link=1676880947
bro.aglt2.org-p1p2-3: 1550653696.612248 recvd=1924106604 dropped=6377813 link=1924106604
bro.aglt2.org-p1p2-4: 1550653696.812188 recvd=1800414436 dropped=4026818 link=1800414436
bro.aglt2.org-p1p2-5: 1550653697.013196 recvd=1815770095 dropped=4173299 link=1815770095
bro.aglt2.org-p1p2-6: 1550653697.213166 recvd=1825038798 dropped=9530017 link=1825038798
```

AGLT2 Net Traffic (1 week)









ELK at AGLT2

- AGLT2 has been using Elasticsearch, Logstash and Kibana for a few years, primarily to host a central syslogging service
- Currently we have a 3 node (all VM) cluster running Elasticsearch 6.5.4 (upgrading to 6.6.0 ASAP)
  - The VMs are hosted on VMware
  - The primary node (atgrid) has 16GB of RAM and 12 cores and runs Logstash and Kibana (avg load 0.66)
  - The secondary nodes (es-1, es-2) are only running Elasticsearch and have 12 GB of RAM and 6 cores
  - Total space available is 3.1 TB (% 69.78 in use)
- Elastic search has **584** indices, **2.477** billion documents and **2544** primary and replica shards as of today (Feb 20, 2019)
- The main data sources are 1) **syslogging** from all our devices, 2) **dCache** logs, 3) **Netflow/Sflow** and 4) **Bro log files**

Netflow/Sflow Monitoring via ELK

- In addition to Bro monitoring we wanted to have better visibility into our network traffic.
- Because we already had an ELK stack, when we heard about ElastiFlow we were intrigued
  - https://github.com/robcowart/elastiflow
  - Install https://github.com/robcowart/elastiflow/blob/master/INSTALL.md
- It was pretty easy to setup. Some challenges getting the sflow-codec and the Kibana elastiflow index imported (maybe better now?)
  - Contact me if you want details!
- Once it was setup we just needed to point our Juniper router to it

Netflow/Sflow Monitoring via ELK (2)

- Setting up our Juniper EX9208 was pretty simple
- The configuration on the right is the bulk of what is needed
- Add additional interfaces as need (those interfaces that connect to the WAN)

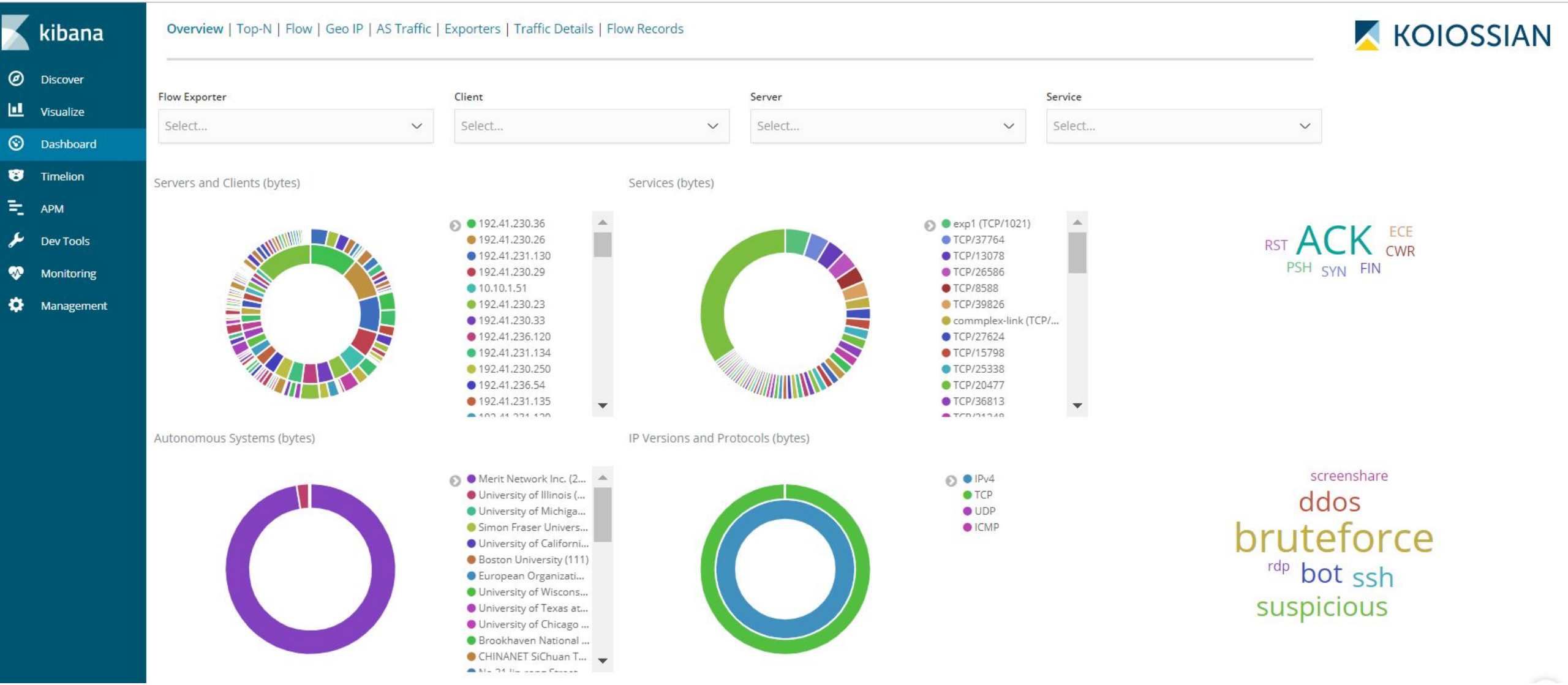
```
sflow {
    agent-id 10.10.1.2;
    polling-interval 1;
    sample-rate {
        ingress 100;
        egress 100;
    }
    source-ip 10.10.1.2;
    collector 10.10.1.9 {
        udp-port 6343;
    }
    interfaces xe-0/0/3.0 {
        polling-interval 1;
        sample-rate {
            ingress 100;
            egress 100;
        }
    }
```

Verify Sflow Setup

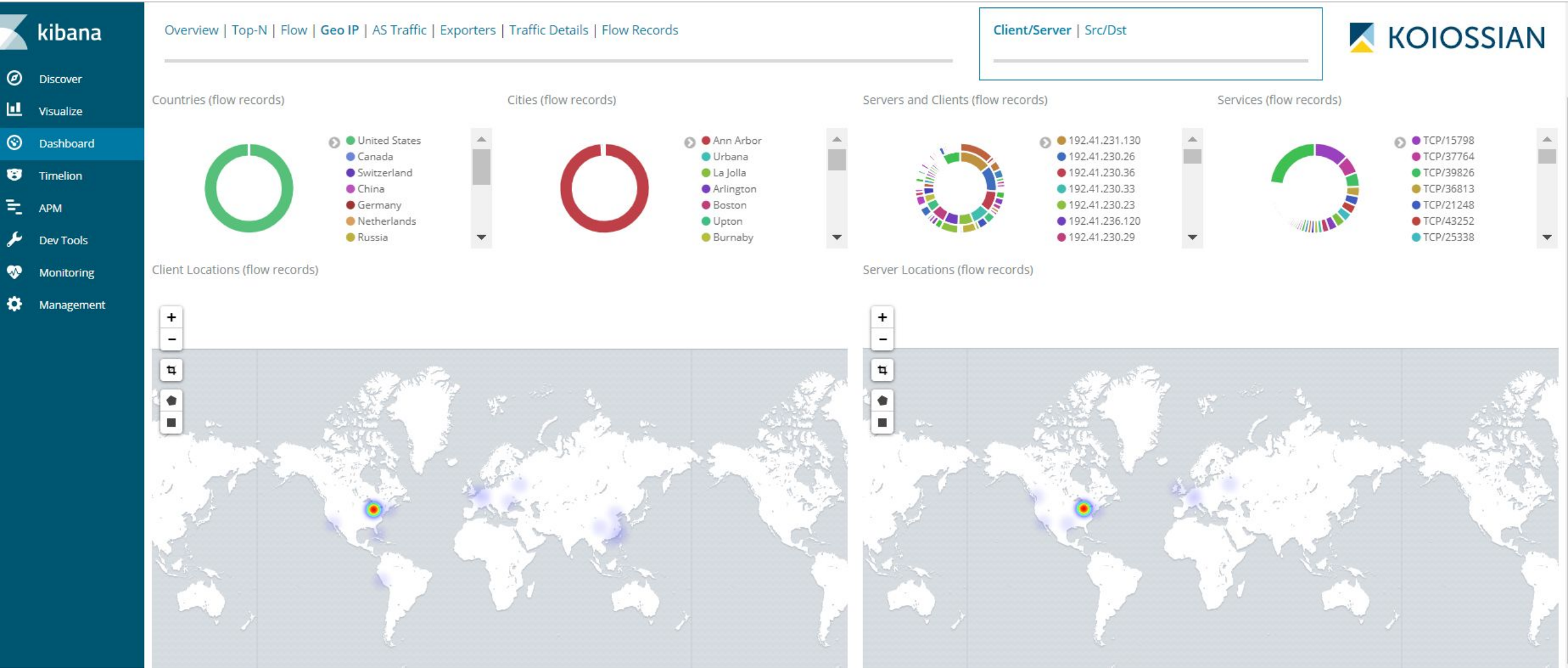
```
admin@shinano-re0> show sflow
sFlow                     : Enabled
Sample limit              : 300 packets/second
Polling interval          : 1 second
Sample rate egress        : 1:100: Enabled
Sample rate ingress       : 1:100: Enabled
Agent ID                  : 10.10.1.2
Source IP address         : 10.10.1.2

{master}
admin@shinano-re0> show sflow interface
Interface         Status              Sample              Adapted             Polling
                                       rate            sample rate           interval

                Egress  Ingress     Egress   Ingress      Egress   Ingress
xe-0/0/3.0       Enabled Enabled    100      100          6400     6400          1
xe-0/1/4.0       Enabled Enabled    100      100          6400     6400          1
xe-0/2/1.0       Enabled Enabled    100      100          6400     6400          1
et-1/0/1.0       Enabled Enabled    100      100          1638400  1638400       1
et-1/2/1.0       Enabled Enabled    100      100          1638400  1638400       1
```

NOTE: Missing IPv6! Need to determine the right setup to also send IPv6 from our border router. (I suspect our EX9208 does NOT support IPv6 SFLow…MX would)

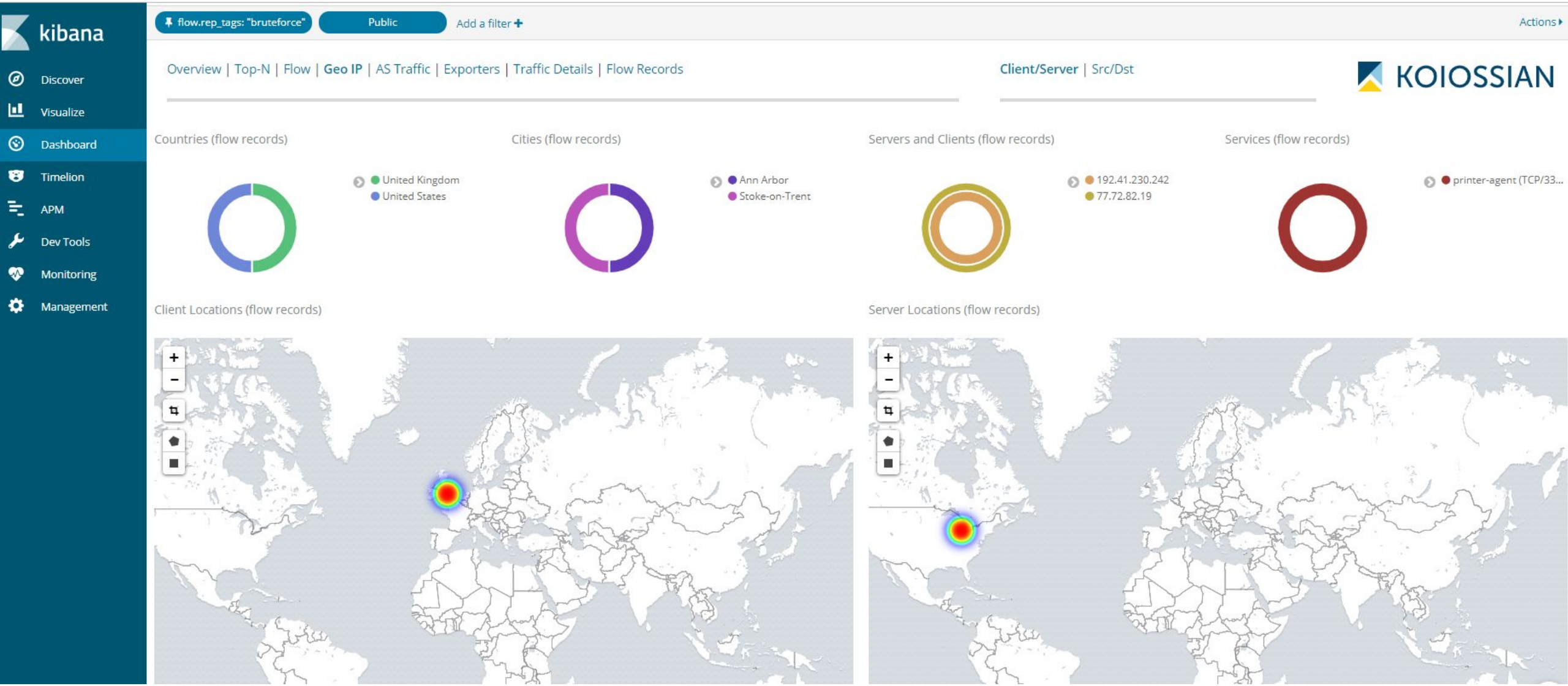
ElastiFlow @ AGLT2 Examples



ElastiFlow @ AGLT2 Examples



ElastiFlow @ AGLT2 Examples



Summary

- New network monitoring with Bro and ElastiFlow providing us with new info; **we need to incorporate it into our operations**
- Our main interest is in configuring some level of alerting when attacks are occurring.
  - Some way to create a report summarizing identified attacks would also be a great addition

Questions ?

OSG SOC Participation

A starting point for discussion…

PATh PARTNERSHIP to ADVANCE THROUGHPUT COMPUTING

HT CENTER FOR HIGH THROUGHPUT COMPUTING

Rising tides

- Immediate benefit to OSG Security from receiving threat intel feeds from the WLCG SOC MISP Instance
- OSG can benefit from working with WLCG SOC efforts to learn what is effective and avoid likely pitfalls
- This is a great tool

What does OSG's participation look like?

- The ET and Council are still discussing but…
- OSG Security will continue to function as a central point for coordinating action between WLCG sites and OSPool
- Short term - consumer of threat data and a revised incident response/coordination role
- Long term - ???

Questions

- What benefits can the other US-ATLAS sites, US-CMS sites, and OSPool sites gain from threat intel?
- Where will effort come from?
- Will small sites be left behind?
  - pDNSSOC - low cost SOC effort using only dDNS data that anyone can participate in
  - Working with campus SOCs
  - beyond?