WLCG SOC Motivation

Shawn McKee / University of Michigan
Why WLCG SOC?

AGLT2 has been concerned about operational security for a long time:

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

USATLAS has also discussed how best to implement security monitoring for its distributed facilities.

WLCG Security Operations Center effort seemed like a good opportunity:

• Provides example best practices, tools and docs
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

Juniper EX9208 Router

Dell R630 Bro Node

Copy of WAN In/Out

WAN via r-BIN-CATH router
MISP UI
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 (Dell R7525) each with two Bluefield-2 NICs (each 2x100G).

Have a milestone for July 2023 to get it into production…
Additional Slides
Connection to Bro Node (1 NIC)
Bro Performance

[output]

[output]

<table>
<thead>
<tr>
<th>Interface</th>
<th>kpps</th>
<th>mbps</th>
<th>(10s average)</th>
</tr>
</thead>
<tbody>
<tr>
<td>bro.aglt2.org/p3p1</td>
<td>70.5</td>
<td>2818.8</td>
<td></td>
</tr>
<tr>
<td>bro.aglt2.org/p3p2</td>
<td>44.1</td>
<td>542.5</td>
<td></td>
</tr>
<tr>
<td>bro.aglt2.org/p1p1</td>
<td>76.1</td>
<td>2939.8</td>
<td></td>
</tr>
<tr>
<td>bro.aglt2.org/p1p2</td>
<td>64.0</td>
<td>328.9</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>254.7</td>
<td>6630.0</td>
<td></td>
</tr>
</tbody>
</table>

[output]
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=1872168099 dropped=6379723 link=1872168099
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-plp1-1: 1550653695.008275 recvd=231878579 dropped=131601959 link=231878579
bro.aglt2.org-plp1-2: 1550653695.208211 recvd=355737802 dropped=71456816 link=355737802
bro.aglt2.org-plp1-3: 1550653695.408198 recvd=275147905 dropped=75679081 link=275147905
bro.aglt2.org-plp1-4: 1550653695.601019 recvd=198015511 dropped=65764347 link=198015511
bro.aglt2.org-plp1-5: 1550653695.80081 recvd=156858519 dropped=63783349 link=156858519
bro.aglt2.org-plp1-6: 1550653696.011028 recvd=283369148 dropped=66690807 link=283369148
bro.aglt2.org-plp2-1: 1550653696.211150 recvd=1859463556 dropped=3611770 link=1859463556
bro.aglt2.org-plp2-2: 1550653696.411283 recvd=1676880947 dropped=2449344 link=1676880947
bro.aglt2.org-plp2-3: 1550653696.612248 recvd=1924106604 dropped=6377813 link=1924106604
bro.aglt2.org-plp2-4: 1550653696.812188 recvd=1800414436 dropped=4026818 link=1800414436
bro.aglt2.org-plp2-5: 1550653697.013196 recvd=1815770095 dropped=4173299 link=1815770095
bro.aglt2.org-plp2-6: 1550653697.213166 recvd=1825038798 dropped=9530017 link=1825038798
```
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)

• Elasticsearch 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
• 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)
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
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…
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?