

---

# Network Threat Detection at the University of Chicago

David Jordan  
on behalf of the UChicago MWT2 Team



11/6/2024



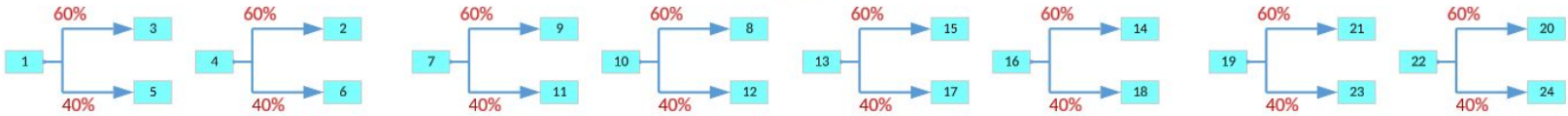
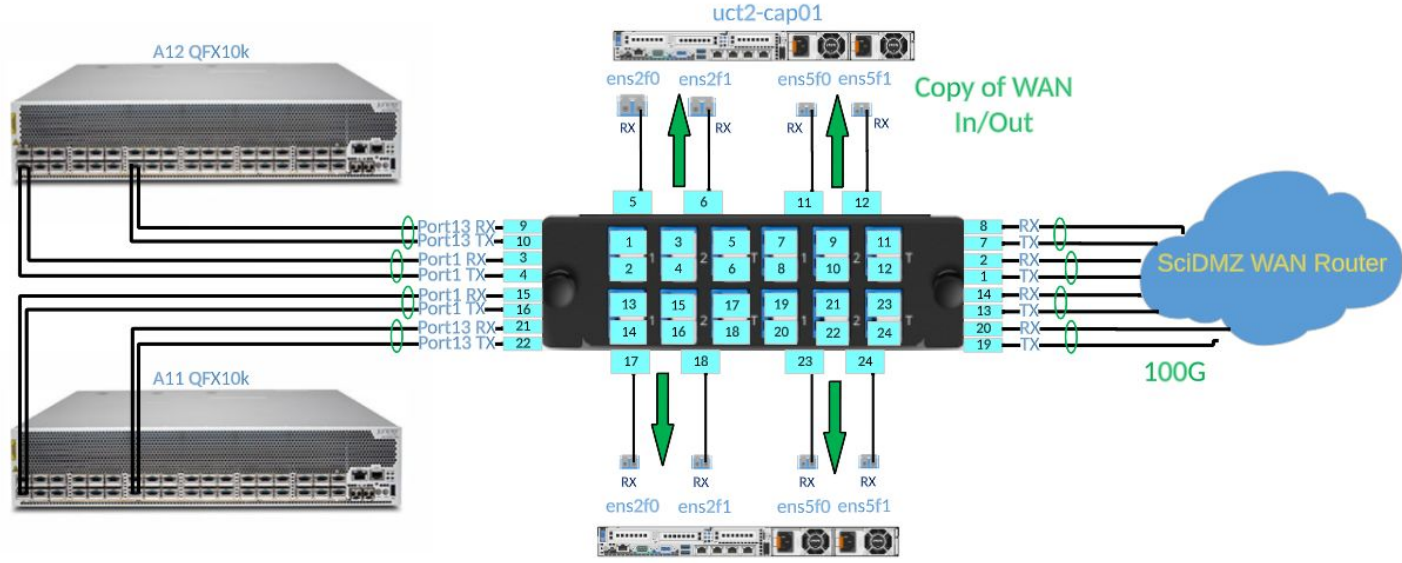
# NetCap equipment at UChicago

---

- 2x bare metal machines for running Zeek w/ 2x 100Gb BlueField-2 NICs, 2x AMD EPYC 74F3 24-Core Processor, and 132GB RAM
- 1x 60/40 LC duplex fiber taps
- 2x Juniper QFX10002 in a virtual router each with 2x100Gb links to the WAN
  - In an active/backup configuration
- One machine per Juniper QFX10k switch in our racks in 6045 S Kenwood Pod-C. Each using half the 60/40 tap
- We purchased the nodes with enough CPU and memory to have multiple processes per interface capturing network traffic and writing output to logs
- Virtual machine running MISP (Malware Information Sharing Platform) on our VM stack

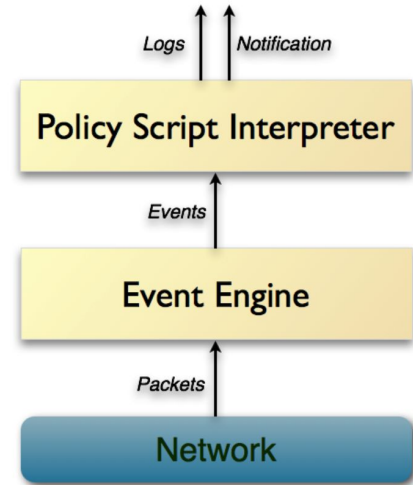


# Setup Diagram



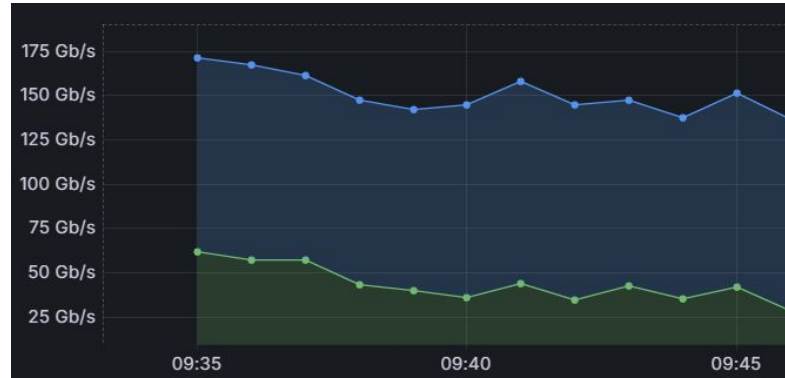
# Our Zeek

- Two bare metal nodes with AlmaLinux 9
  - uct2-cap01.mwt2.org & uct2-cap02.mwt2.org
- Configured as a Zeek cluster with cap01 as the manager
- BlueField-2 NICs only used for capturing data
  - A separate 10Gb link is used for normal access
- Zeek Release 6.0.0
- 12 processes per interface capturing data (48 per node)
  - Each capture process has own dedicated core



# Some problems with the capture

- Zeek reports 1/10th the traffic our SNMP switch monitoring does
  - Zeek possibly reporting only header size?
- Fiber split can cause extra dropped packets and issues
  - Tried 70/30 split first, but needed 60/40 for better capture



```
[root@uct2-cap01 ~]# zeekctl capstats
Interface      kpps      mbps      (10s average)
-----
uct2-cap01.mwt2.org/af_packet: :ens2f0  116.2     1225.5
uct2-cap01.mwt2.org/af_packet: :ens2f1  264.8     2444.6
uct2-cap01.mwt2.org/af_packet: :ens5f0  108.5     1167.2
uct2-cap01.mwt2.org/af_packet: :ens5f1  170.9     1386.4
uct2-cap02.mwt2.org/af_packet: :ens2f0  210.6     2113.1
uct2-cap02.mwt2.org/af_packet: :ens2f1  146.7     1684.8
uct2-cap02.mwt2.org/af_packet: :ens5f0  222.8     2301.1
uct2-cap02.mwt2.org/af_packet: :ens5f1  152.9     1768.2

Total          1393.4    14090.900000000001
```



# Using Zeek Intel

```
[root@uct2-cap01 ~]# ll /opt/zeek/intel/
total 11765
-rw-r--r-- 1 root root      90 Sep 25 14:00 certhash.txt
-rw-r--r-- 1 root root    7251 Sep 25 14:00 domain.txt
-rw-r--r-- 1 root root      90 Sep 25 14:00 email.txt
-rw-r--r-- 1 root root 7512330 Sep 25 14:00 filehash.txt
-rw-r--r-- 1 root root    3589 Sep 25 14:00 filename.txt
-rw-r--r-- 1 root root   17948 Sep 25 14:00 ip.txt
-rw-r--r-- 1 root root      90 Sep 25 14:00 software.txt
-rw-r--r-- 1 root zeek    207 Sep 25 08:56 test2.txt
-rw-r--r-- 1 root root    215 Sep 25 11:15 test.txt
-rw-r--r-- 1 root root 4302417 Sep 25 14:00 url.txt
[root@uct2-cap01 ~]# |
```

```
[root@uct2-cap01 ~]# cat /opt/zeek/intel/test.txt
#fields indicator      indicator_type  meta.source      meta.desc          meta.url          meta.do_notice  meta.if_in
67.176.240.185 Intel::ADDR     Manual Test intel   test-url.mwt2.org T -
192.170.231.213 Intel::ADDR     Manual Test intel   test-url.mwt2.org T -
```

## local.zeek

```
redef Intel::read_files += {
# MISP feeds
  "/opt/zeek/intel/domain.txt",
  "/opt/zeek/intel/email.txt",
  "/opt/zeek/intel/filehash.txt",
  "/opt/zeek/intel/filename.txt",
  "/opt/zeek/intel/ip.txt",
  "/opt/zeek/intel/url.txt",
  "/opt/zeek/intel/test.txt",
};
```



# Zeek Intel Hits

```
[root@uct2-cap01 ~]# cat /root/test-zeek-logs/intel.log
#separator \x09
#set_separator ,
#empty_field (empty)
#unset_field -
#path intel
#open 2023-09-25-15-32-32
#fields ts uid id.orig_h id.orig_p id.resp_h id.resp_p seen.indicator seen.indicator_type seen.w
here seen.node matched sources fuidd file_mime_type file_desc
#types time string addr port addr port string enum enum string set[enum] set[string] string string
string
1695652764.576800 Cr8m04kmfcPNEfuZ 192.170.231.213 60224 192.170.240.8 22 192.170.231.213 Intel::ADDR Conn::
IN_ORIG zeek Intel::ADDR Manual - -
1695652782.301889 CGFleT1wWN1u6fscF9 192.170.231.213 60226 192.170.240.8 22 192.170.231.213 Intel::ADDR Conn::
IN_ORIG zeek Intel::ADDR Manual - -
1695652783.772364 CAESIn1m9ciZtKKbpd 192.170.231.213 60228 192.170.240.8 22 192.170.231.213 Intel::ADDR Conn::
IN_ORIG zeek Intel::ADDR Manual - -
#close 2023-09-25-15-32-33
```

---

Hits on 192.170.231.213 based on the test.txt file fed into Zeek with Intel::read\_files

---



# Zeek Notify

```
[root@uct2-cap01 ~]# cat /root/test-zeek-logs/notice.log
#separator \x09
#set_separator ,
#empty_field (empty)
#unset_field -
#path notice
#open 2023-09-25-15-32-32
#fields ts uid id.orig_h id.orig_p id.resp_h id.resp_p fuid file_mime_type file_desc proton
ote msg sub src dst p n peer_descr actions email_dest suppress_for remote_location.countr
y_code remote_location.region remote_location.city remote_location.latitude remote_location.longitude
#types time string addr port addr port string string string enum enum string string addr addr port c
ount string set[enum] set[string] interval string string string double double
1695652764.576800 Cr8m04kmfcPNEfuZ 192.170.231.213 60224 192.170.240.8 22 - - - tcp Intel:
:Notice Intel hit on 192.170.231.213 at Conn::IN_ORIG Indicator = 192.170.231.213 192.170.231.213 192.170.240.8 22 - N
otice::ACTION_LOG,Notice::ACTION_EMAIL djordan66@uchicago.edu,(empty) 43200.000000 - - - -
#close 2023-09-25-15-32-33
```

---

Only one notification per indicator hit per 12hrs to limit spam (configurable)

---





gardnergrouperquest@lists.uchicago.edu on behalf of Zeek<zeek@uct2-cap01.mwt2.org>



To: gardnergrouperquest@lists.uchicago.edu

Tue 11/5/2024 5:03 PM

Message: Intel hit on 213.32.39.47 at Conn::IN\_ORIG

Sub-message: Indicator = 213.32.39.47

Connection: 213.32.39.47:60017 -> 192.170.240.138:22

Connection uid: ClpWsh2VYR8M46nDQ3

### Email Extensions

#### Service:

Description: Cyber attack on the mail server of a state service to exfiltrate data. Network Indicators

URL: [https://urldefense.com/v3/\\_https://uct2-misp.mwt2.org:443/events/view/6725\\_!!BpyFHLRN4TMTrA!9Qv6vGe\\_cAo2EJZWmMUeQEOv\\_a-QjHaQYpMPQhYgMp1VFJvFKYwkSkVJSraY\\_bBVKLnUqqWxkqKvOXi0xE5A8U8fCwx9Lg\\$](https://urldefense.com/v3/_https://uct2-misp.mwt2.org:443/events/view/6725_!!BpyFHLRN4TMTrA!9Qv6vGe_cAo2EJZWmMUeQEOv_a-QjHaQYpMPQhYgMp1VFJvFKYwkSkVJSraY_bBVKLnUqqWxkqKvOXi0xE5A8U8fCwx9Lg$)

Intel source: MWT2 MISP (9b1c7d67-da24-4f73-bd67-07fe721571b4) - Security Service Ukraine

resp/dst hostname: c023.af.uchicago.edu

orig/src hostname: kiana.probe.onyphe.net

Intel hit on one of our AF nodes from yesterday!



# Our MISP Instance

---

- Runs on a VM on our OpenStack cluster
- The MWT2 instance connects with CERN's to pull threat intelligence they have
  - Must have access to the other instance and use an API key
- MFA required to login by default
- Currently do not publicly publish any events or threats from the MWT2 instance
- Installed and running via docker containers
  - <https://github.com/JiscCTI/misp-docker>

# MISP Web Portal

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API ★ MISP DJordan66 Log out

List Events  
Add Event  
Import from...  
REST client

List Attributes  
Search Attributes

View Proposals  
Events with proposals  
View delegation requests  
View periodic summary

Export  
Automation

## Events

« previous next »

Event info Filter

<input type="checkbox"/>	Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Distrib
<input type="checkbox"/>	✓ MWT2	MWT2	39			4		djordan66@uchicago.edu	2023-09-18	Test event for MISP to Zeek integration and alerting	All
<input type="checkbox"/>	✓ GovCERT	MWT2	6		Phishing ttp:green	19		djordan66@uchicago.edu	2023-08-18	Microsoft credential phishing using QR codes	Organic
<input type="checkbox"/>	✓ CERT-EE_8833	MWT2	3	Attack Pattern	Phishing ttp:green	2		djordan66@uchicago.edu	2023-08-20	Phishing URL findings	All
				Input Capture - T1056							
				Phishing - T1566							
<input type="checkbox"/>	✓ CERT-EE_8833	MWT2	4	Attack Pattern	Phishing ttp:green	2	1	djordan66@uchicago.edu	2023-08-20	Phishing URL findings	All
				Input Capture - T1056							
				Phishing - T1566							
<input type="checkbox"/>	✓ CERT-EE_8833	MWT2	5	Attack Pattern	Phishing ttp:green	2	1	djordan66@uchicago.edu	2023-08-20	Phishing URL findings	All
				Input Capture - T1056							
				Phishing - T1566							

# Elasticsearch (for Zeek)

---

- Distributed RESTful search and analytics engine
- Robust clusterization and easily scalable
  - Supported to run on the cloud (elastic cloud) or dedicated hardware
- Can enrich the data with processing and analytic tools (e.g. GeoIP)
- Has built in [Zeek integration](#)
  - Need to install an “elastic-agent” service on the host with the logs
- Extensive documentation

# Our Elasticsearch (regarding Zeek)

---

- 24x nodes in the cluster
  - 17 data nodes for storage
  - 5 head nodes
  - 1 ingress and kibana host
  - 1 dedicated ingress node (not currently active)
- Elastic-agent installed on uct2-misp and uct2-cap01 to send MISP and Zeek data respectively to elasticsearch through the ingress host
- Processes the Zeek connection logs to break down % of connection types, most popular hosts, etc.
- Uses GeoIP to map the connections that come through our network on the dashboard





All Connection Destinations outside UChicago MWT2 network 10/4/23–10/11/23



## XrootD (port 1094) and WebDav Traffic (port 8443) 10/4/23–10/11/23



# Summary and Next Steps

---

- Zeek and MISP (Malware Information Sharing Platform) are installed and configured at UChicago
- Zeek configured to alert based on intel hits
- Our MISP pulls data from CERN's central instance
  - Zeek then grabs this data from the MWT2 MISP instance via a cron
- Elasticsearch copies Zeek logs and processes data
  - Continue elasticsearch data enrichment
    - Working with OSG Security to allow them to use/analyze our data
- Understand holes in monitoring and data capture

Questions?