Network Threat Hunter Training

Level 1

Thank you to our sponsors!

ACTIVE | COUNTERMEASURES

You'll need the class VMs

You only need one of these!
They are all the same, just tweaked for different platforms.

Hash is SHA256

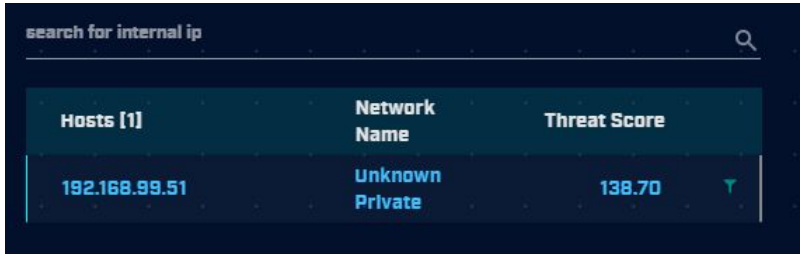
VirtualBox
https://thunt-level1.s3.amazonaws.com/vbox-thunt-L1-202308.zip
5CF82AAEA859F9297CB33569BCFDC5023CAB87E78BD7605C82844D65BB41B899
Generic OVF
https://thunt-level1.s3.amazonaws.com/ovf-thunt-L1-202308.zip
D210F54CDC3E425E10C8FF66AE7F9B1EF0AC5924CE6A5543E1DDDC765252F992
VMware
https://thunt-level1.s3.amazonaws.com/vmware-thunt-L1-202308.zip
57E63852D10BC3C0D9F5B86E369FEFA555D8BF6B6ADA5D31A3E175F9B5109144

If you can't download the VM

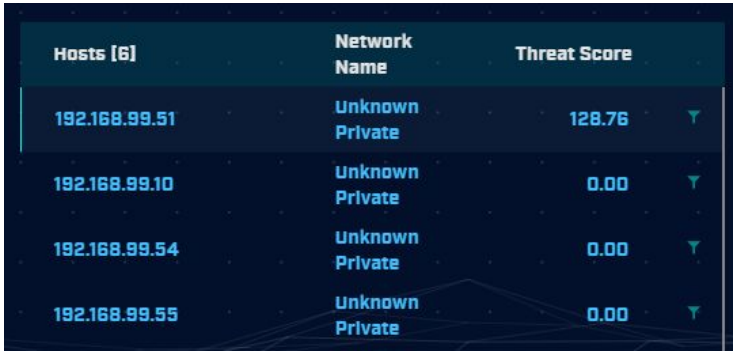
- We have a new online option
- Public facing AC-Hunter server
- Read only access
- You **cannot**:
  - Add/delete databases
  - Add/delete safelists
  - Work at the command line
- Older version so experience is slightly different
- VM preferred but better than no option
- See the FAQ in #acm-webcast-content

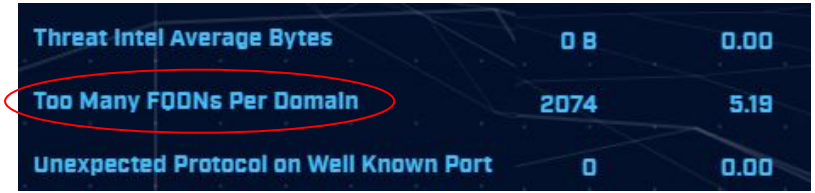
VM versus online

VM



Online





VMWare/VirtualBox host access

- VMWare VM accessed via IP address
  - Originally set to 192.168.149.128
  - Example: ssh threat@192.168.149.128
  - Point host browser at https://192.168.149.128
- VirtualBox VM accessed via loopback
  - You must setup port forwarding & reboot!
  - Example: ssh threat@127.0.0.1:10022
  - Point host browser at https://127.0.0.1:10443

Logging in

- Using the class VM to do the labs
  - Console & UI login info
    - Name: threat
    - Pass: hunting
  - Same login info when using SSH
  - Web browser interface to ACH CE
    - Name: threat@activecountermeasures.com
    - Pass: hunting2
- Public servers have Web UI only
- Q&A in Discord

VMWare Troubleshooting

- Guest will not start
- Error "VM using a hardware version that is not supported"
- Right click VM
  - Manage → Change hardware compatibility
  - Follow Wizard → Pick your VMWare product

https://www.augmastudio.com/2023/02/05/fix-virtual-machine-is-using-a-hardware-version-that-is-not-supported/

VMWare troubleshooting (2)

- Problem: On VMWare, I can't connect to the IP address in the slide
- Root cause: Sometimes VMware changes the host portion of the address
- Open terminal and run this command:

```
ip address | grep 192.168.149
```

VMWare generic problems

- VMWare loves to consume memory
- VMWare loves to consume vCPUs
- Feed the beast!
- This seems to fix a lot of problems

VirtualBox troubleshooting

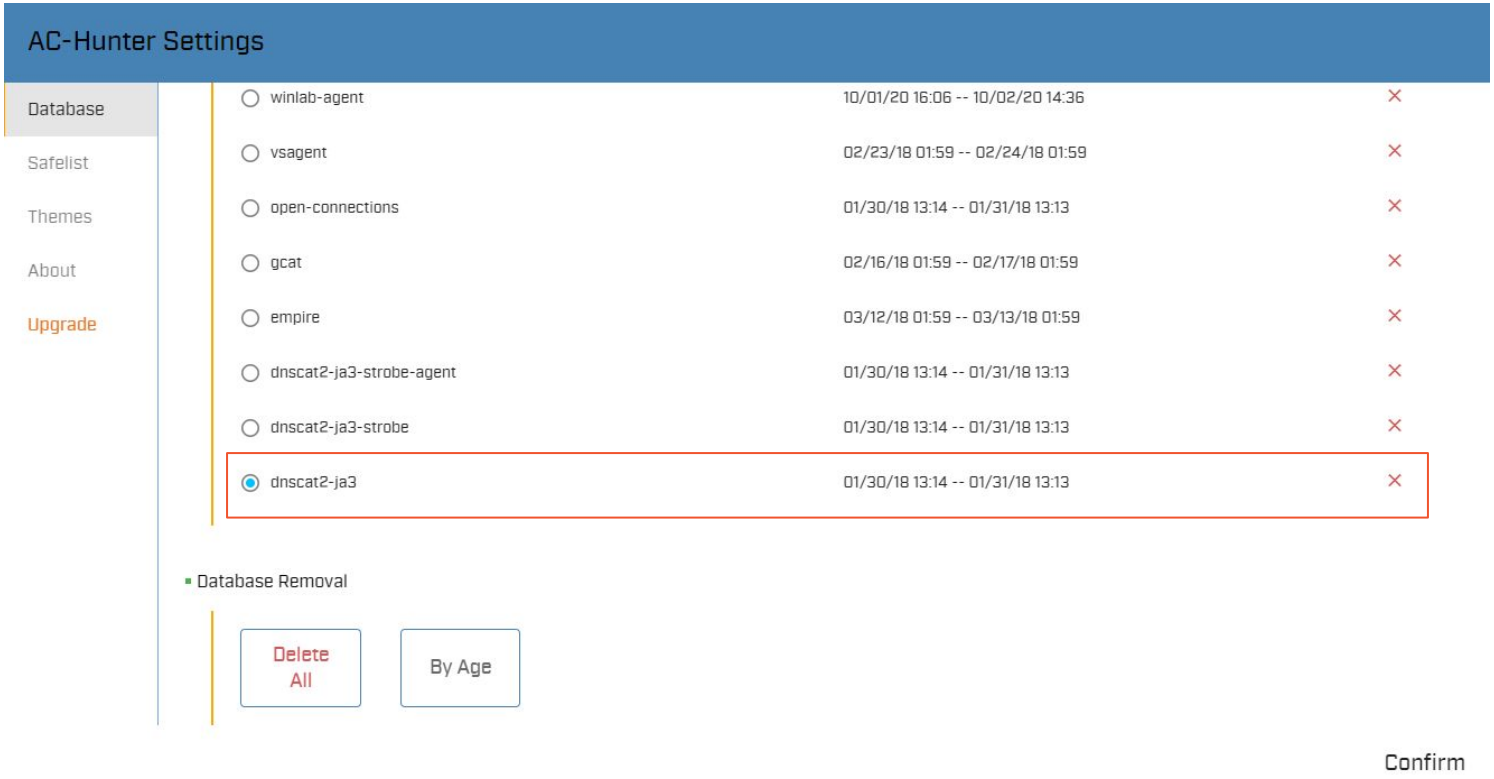
- Can't connect to VM from host via loopback address
- Possible IP change when imported
- Open terminal and run this command:

```
ip address | grep 10.0.2
```

- Follow these instructions but using IP you saw when running the above command

https://www.activecountermeasures.com/port-forwarding-with-virtualbox/

Which ACH CE database to load?



<shameless_plugs>

New bash scripting class!

- Authored by the ONE… the ONLY… Bill Stearns
- Getting comfortable with Linux command line
- Bash scripting
- Managing Linux systems with it
- Automating tasks
- Available on-demand

https://www.antisyphontraining.com/on-demand-courses/bash-scripting-for-server-administration-w-bill-stearns/

Classes I'm teaching

- Intro to Packet Decoding
  - IP headers from a security perspective
  - April 23rd - 26th
  - https://www.antisyphontraining.com/live-courses-catalog/getting-started-in-packet-decoding-chris-brenton/
- Advanced Threat Hunting
  - Next step up from this course, mostly C2 labs
  - May 21st - 24th, then Aug 13th - 16th
  - https://www.antisyphontraining.com/advanced-network-threat-hunting-w-chris-brenton/
- Security Compliance and Leadership
  - Getting funded, C level communications, team management
  - Aug 22nd & 23rd, to be announced on Antisyphon site
  - https://www.antisyphontraining.com/live-courses-catalog/security-leadership-and-management-w-chris-brenton/
- Next run of this class is…TBD

</shameless_plugs>

Logistics

- 10 minute break at top of each hour
- 20 minute break at 3 hour point
- Use the Discord channel for discussion
  - #acm-webcast-chat channel
- The team is monitoring for your questions

Help with command line syntax

- We'll be working at the command line
- Some are nested commands

```
<command> | <command> | <command>
```

- I'll explain what's going on
- Try adding one command at a time to observe how it changes the output

https://www.explainshell.com/

Goals for this class

- Define "cyber threat hunting"
- Identify how to perform a threat hunt
- Define and identify connection persistency
- Learn how to investigate endpoints
- Hands on lab time running down real C2 channels used in the wild

What is threat hunting?

- Actively searching your environment for compromised systems
- Triggered by time or process, not by alerts
- Validate the integrity state of every system
  - Not just desktops and servers
  - Not just systems submitting logs to your SIEM
  - Not just the patterns you can hypothesise
- Output is a compromise assessment

Are we getting better at detection?

- Interesting Mandiant M-Trends nuggets
  - External detection at 6 year high
  - 55% in US, 74% in EMEA
  - 67% of ransomware goes undetected
- Dwell time down to less than 30 days
  - But ***drop shows no correlation to breach impact***
  - Skewed by Ransomware at 5 days
  - This questions if detection is actually improving

https://inthecloud.withgoogle.com/mandiant-m-trends-2023/download.html

But I hunt my SIEM...

- You don't see everything
- Using data from compromised host
- Do you spend your time "hunting" or tuning the SIEM?
- Most security frameworks require SIEM
- And yet we are seeing no improvement
- Not the silver bullet we thought it was

https://www.activecountermeasures.com/check-the-stats-your-threat-hunting-is-probably-broken/

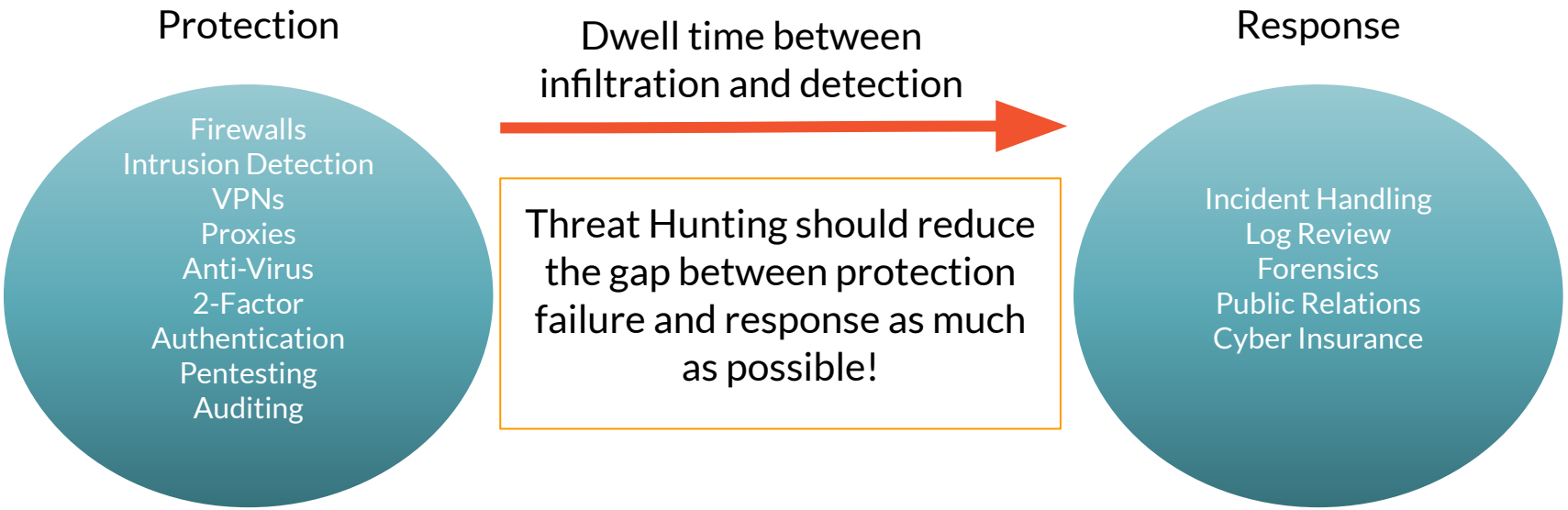
But AI will fix it, right?

- AI is vaporware and just a marketing term
- What we really have is machine learning
  - Machines do not always "learn" what we want
  - Unexpect bias in the datasets due to lack of real intelligence
  - Neural network AI is extremely challenging to troubleshoot
- Deployment is exceeding our ability to improve
  - Results are not always logical (black and asian nazis)
  - Sometimes they lie a lot (will make up data and news)
  - Write haiku's flaming their owners (can be lead astray)
  - Run over and drag pedestrians (yes this has happened)
  - Run polls to guess the cause of death (no real intelligence means no empathy)
  - Need to remove features to not be racist (this is just sad)
  - Teach kids how to make their disorder worse
  - Diagnose tuberculosis based on age of MRI machine
- If it fails in security, how long before you can tell?

Disclaimer - This is new territory

- Threat hunting has no industry standards
- You are getting in on the ground floor! ;-)
- We are still working out best processes
- This content is based on our experiences
  - Literally thousands of threat hunts
  - Scales through various environment sizes
  - Identifying new attacks that other processes miss
  - Thus this content will change over time

The Purpose of Threat Hunting



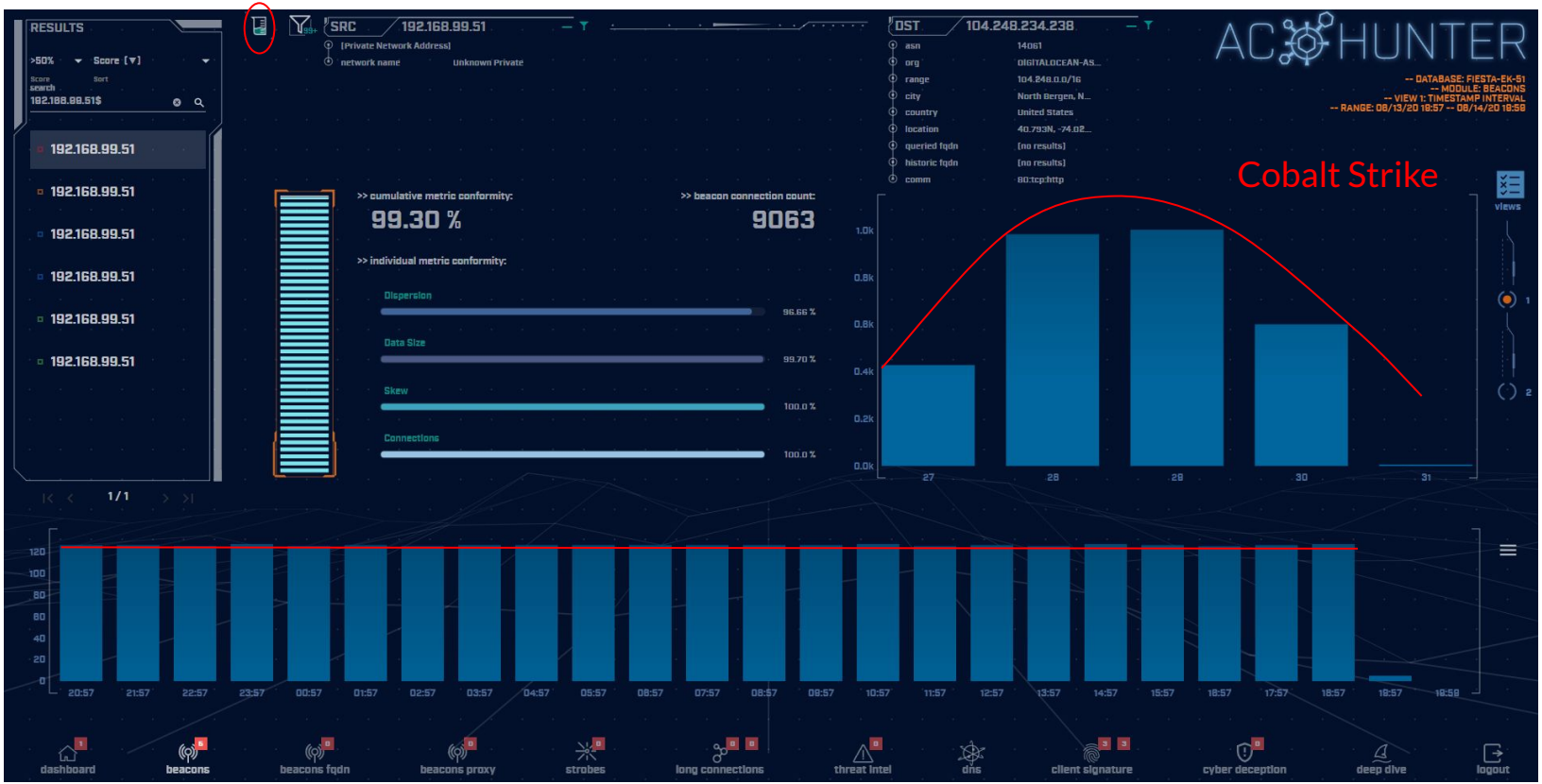
Start with the network

- The network is the great equalizer
  - You see everything, regardless of platform
  - Desktop, servers, IIoT, etc all reviewed the same
- You can hide processes but not packets
- Malware is usually controlled
  - Which makes targeting C2 extremely effective
  - Identify compromise when C2 "calls home"
  - Must be frequent enough to be useful
- Wide view so you can target from there

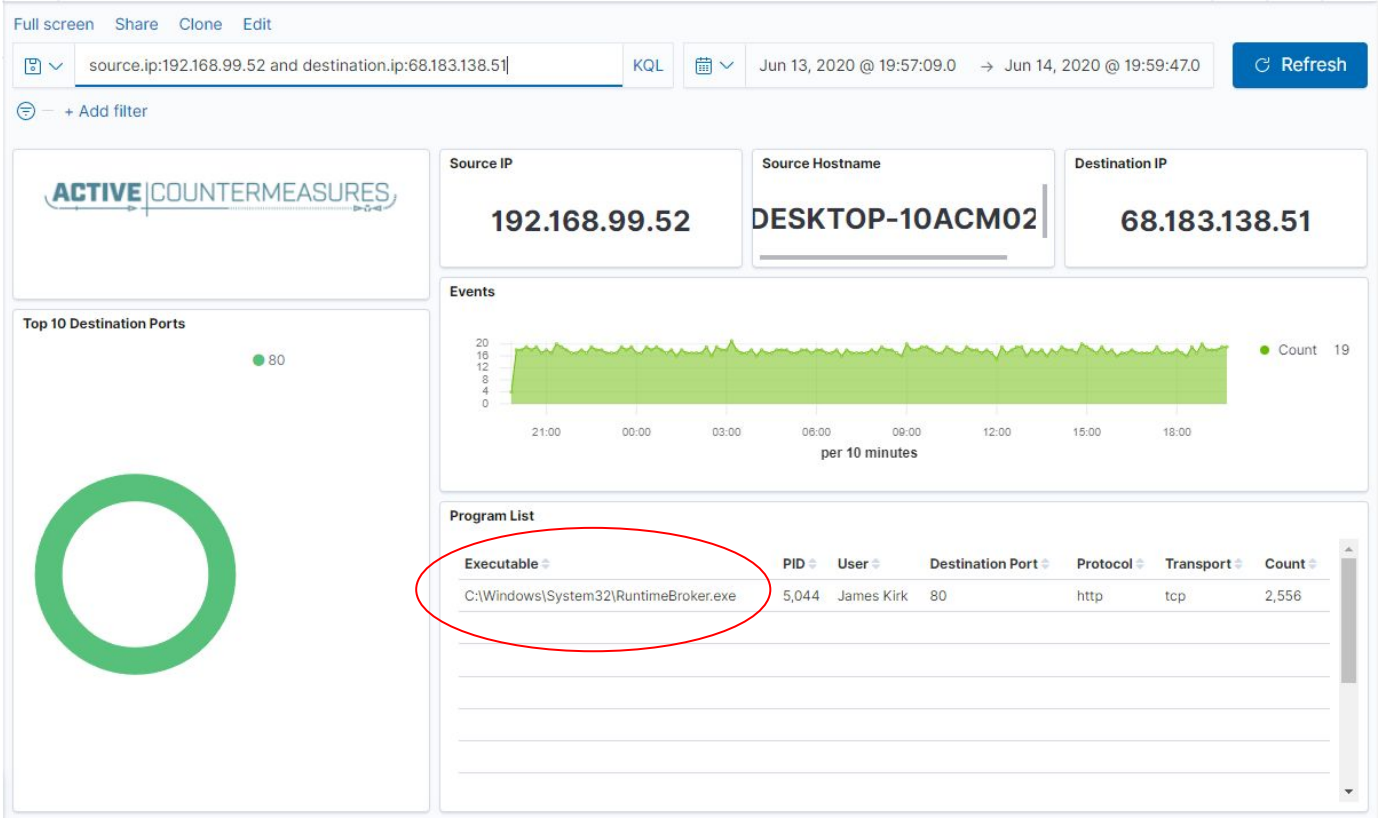
The threat hunting process

- Identify connection persistency
- Business need for connection?
  - Reputation check of external IP
- Abnormal protocol behaviour
- Investigation of internal IP
- Disposition
  - No threat detected = add to safelist
  - Compromised = Trigger incident handling

Start on the network



THEN pivot to the system logs



Don't cross "the passive/active line"

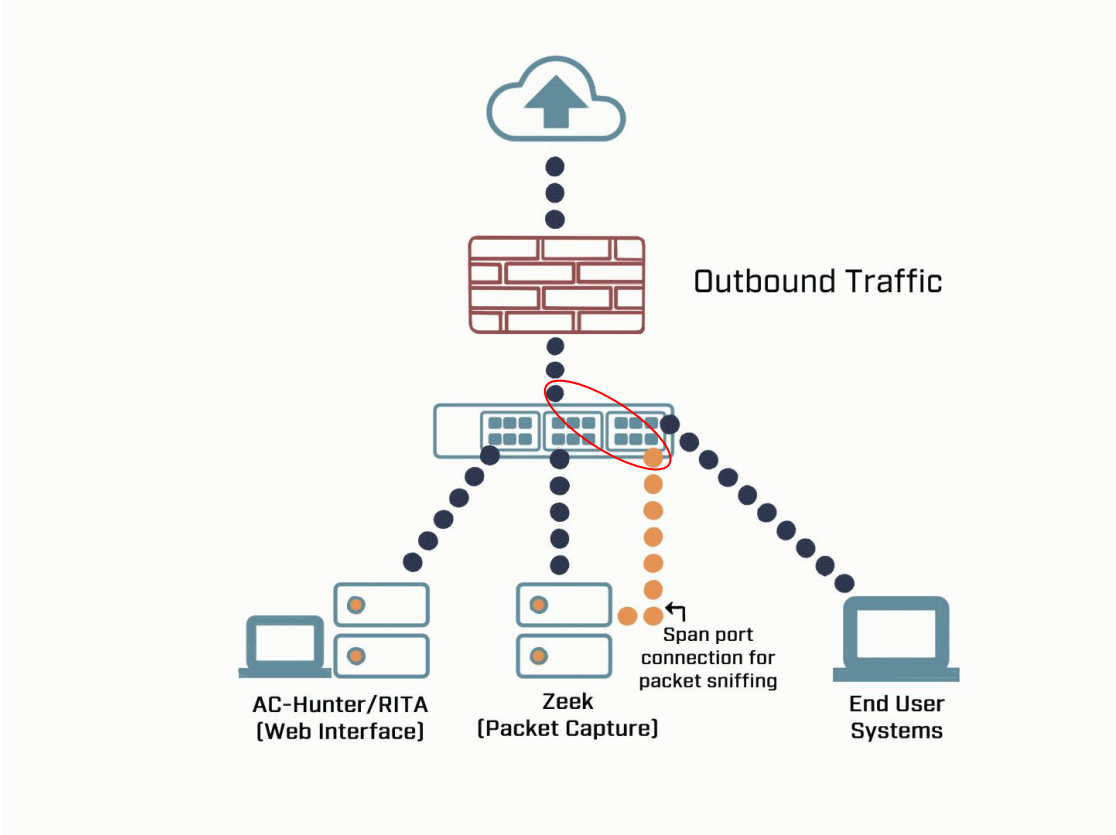
- All threat hunting activity should be undetectable to an adversary
- Passive in nature
  - Review packets
  - Review SIEM logs
- If active techniques are required, we should trigger incident response first
  - Example: Isolating the suspect host
  - Example: Running commands on suspect host

C2 Detection Techniques

Where to Start

- Traffic to and from the Internet
  - Monitor internal interface of firewall
- Packet captures or Zeek data
- Analyze in large time blocks
  - More data = better fidelity
  - Minimum of 12 hours, 24 is ideal
- Analyze communications in pairs
  - Every outbound session passing the firewall
  - Ignore internal to internal (high false positive)

Typical deployment



Does targeting C2 have blind spots?

- Attackers motivated by gain
  - Information
  - Control of resources
- Sometimes "gain" does not require C2
  - Just looking to destroy the target
  - Equivalent to dropping a cyber bomb
  - We are talking nation state at this level
- NotPetya
  - Worm with no C2 designed to seek and destroy
  - These are rare as they frequently go sideways

Start by checking persistency

- Focus on persistent connections
  - Internal system in constantly initiating connections with an outside "system"
  - Long connections
  - Beacons
- Persistent connections should have an identifiable business need
  - Checking the time
  - Checking for patches

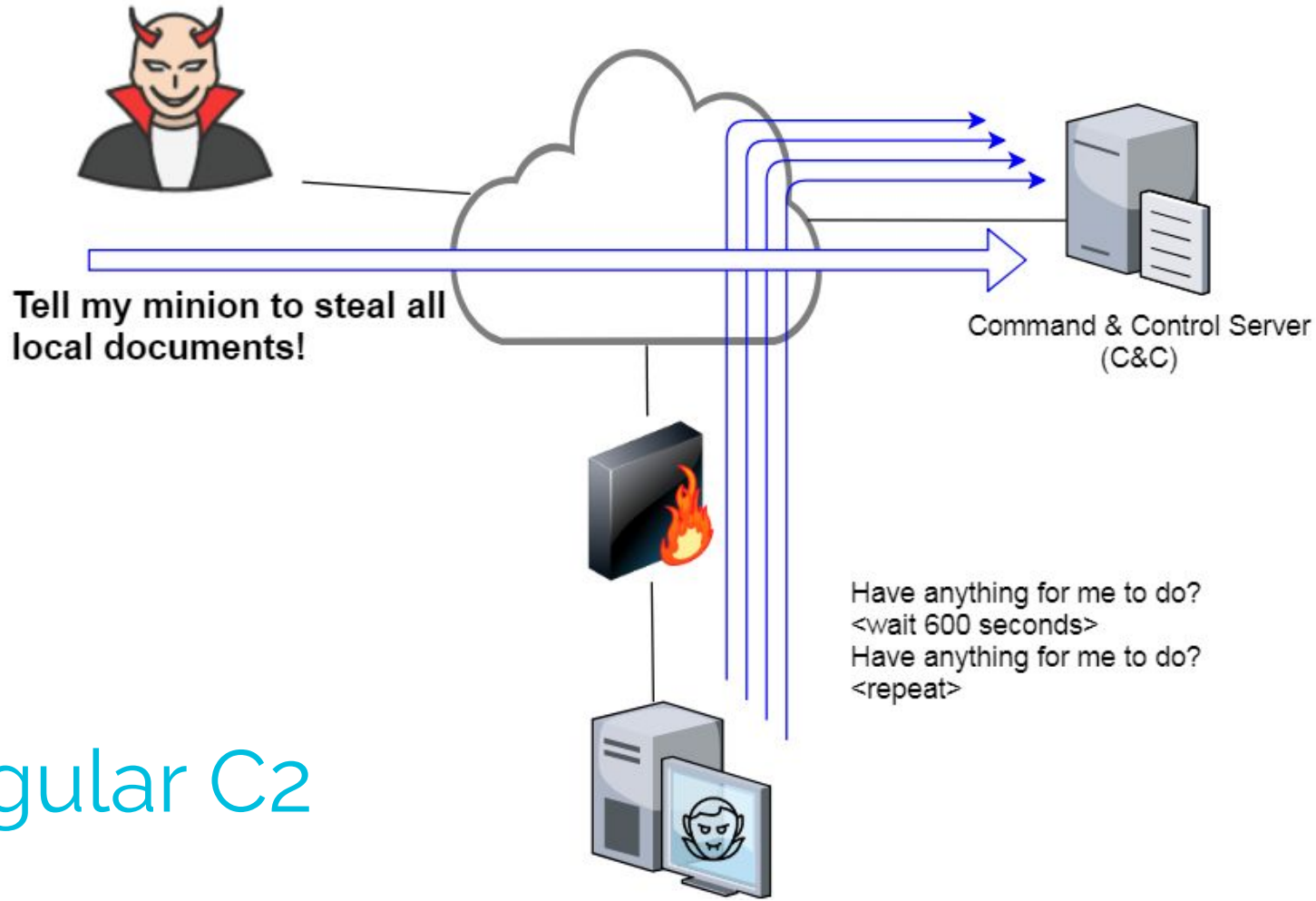
Long connections

- You are looking for:
- Total time for each connection
  - Which ones have gone on the longest?
- Cumulative time for all pair connections
  - Total amount of time the pair has been in contact
- Can be useful to ignore ports or protocols
  - C2 can change channels

Long connection example

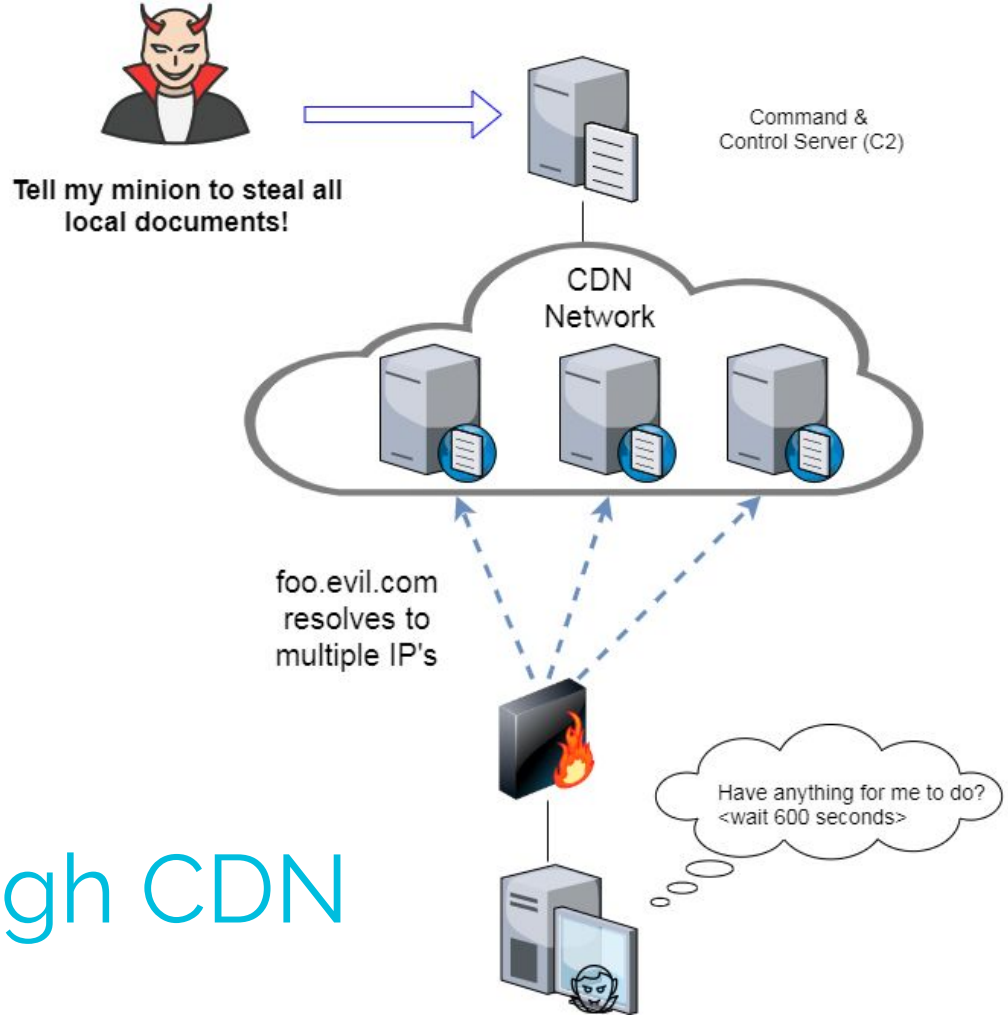
What is a beacon?

- Repetitive connection establishment between two IP addresses
  - Easiest to detect
- Repetitive connection establishment between internal IP and FQDN
  - Target can be spread across multiple IP's
    - Usually a CDN provider
  - Target IPs also destination for legitimate traffic
  - Far more difficult to detect


Tell my minion to steal all local documents!
Command & Control Server (C&C)
Have anything for me to do?
<wait 600 seconds>
Have anything for me to do?
<repeat>

Regular C2

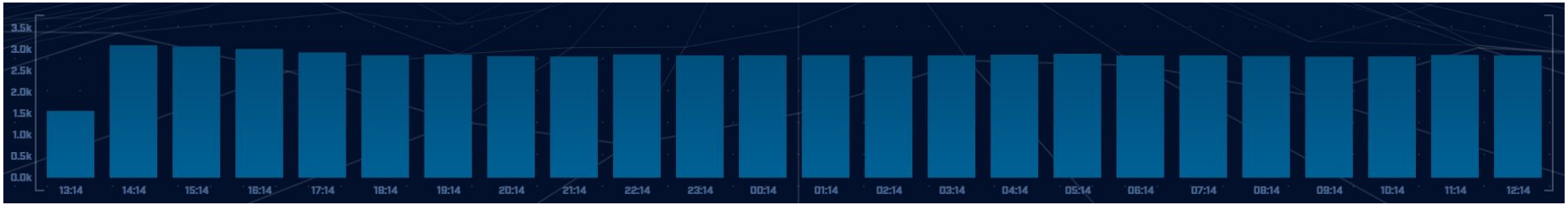
C2 through CDN



Beacon detection based on timing

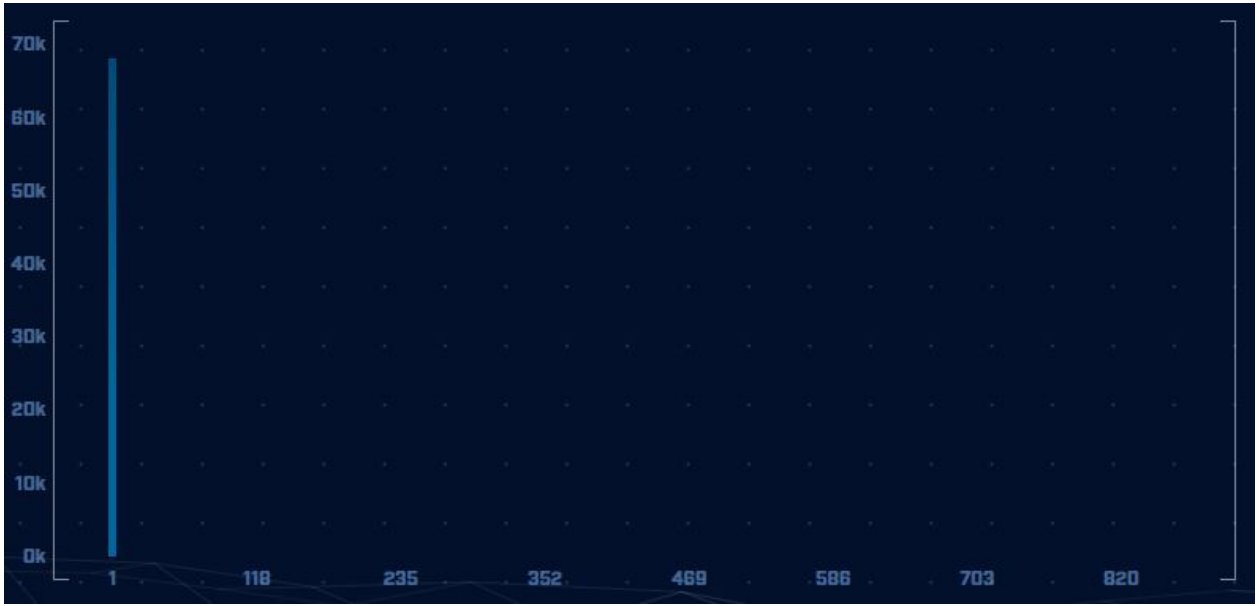
- May follow an exact time interval
  - Technique is less common today
  - Detectable by k-means
  - Potential false positives
- May introduce "jitter"
  - Vary connection sleep delta
  - Avoids k-means detection
  - False positives are extremely rare
- Short enough delta for terminal activities

Connection quantity VS time



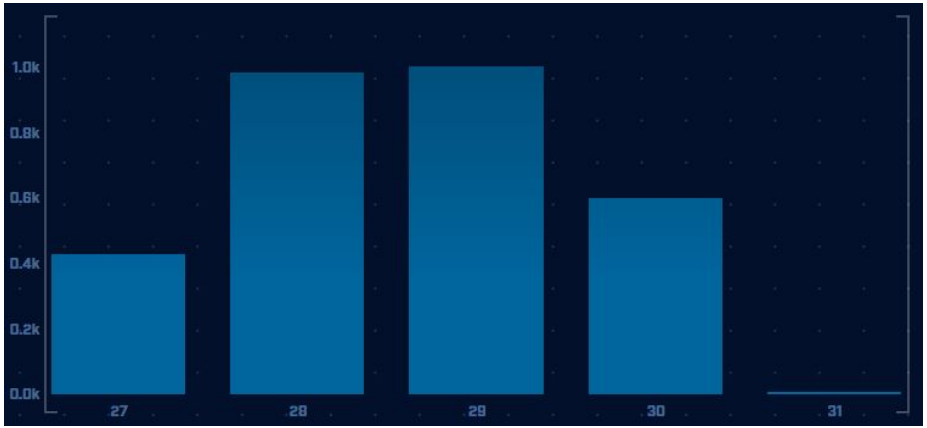
Each bar represents the number of times the source connected to the destination during that one hour time block

Connect time deltas with no jitter



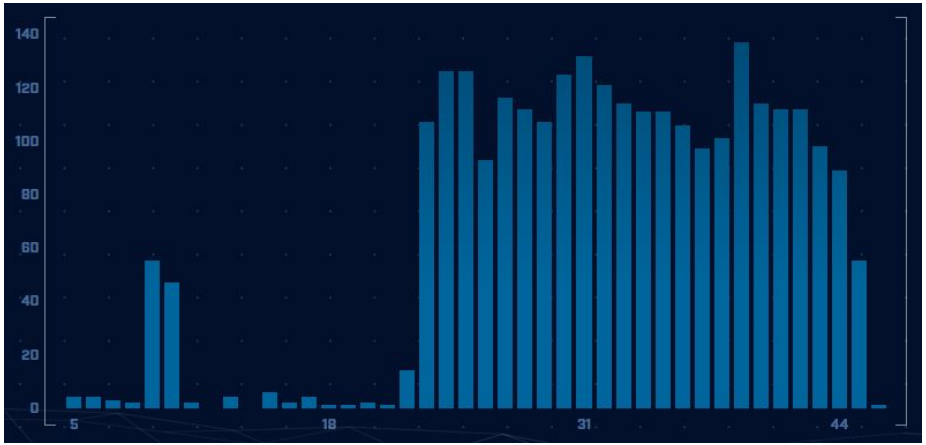
How often a specific time delta was observed

Connection time deltas with jitter



Cobalt Strike will typically produce a bell curve

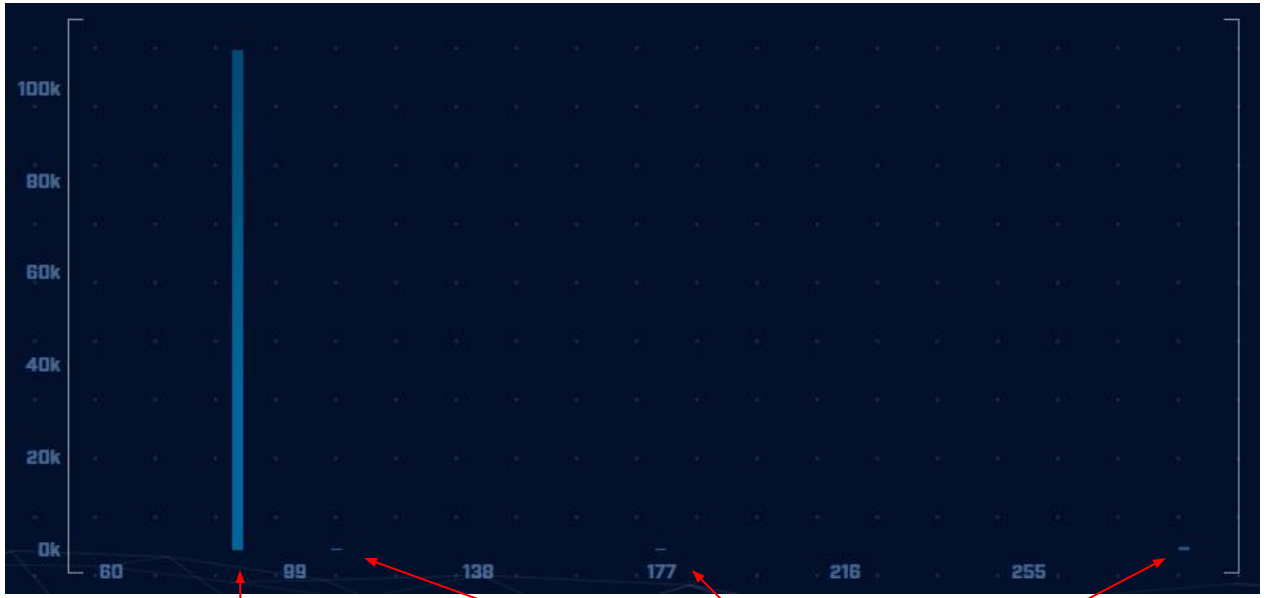
Pretty well randomized but still a small dwell time "window"



Detection based on session size

- Focuses on detection of the heartbeat
  - Useful for C2 over social media
- Variations from the heartbeat indicate activation of C2 channel
- Session size can help reveal info regarding commands being issued
- Possible to randomly pad but this is extremely rare

Session size analysis



Safelisting

- Not all persistence is "evil"
- Could be part of normal operations
  - Keep computer time in sync
  - Checking for patches
  - Checking on an external service
- When business need can be identified, we should safelist the connection
  - Keep it out of future hunts
  - Don't make safelists any broader than necessary

Identifying business need

- Do you recognize the domain?
  - microsoft.com
  - windows.com
  - ntp.org
- Can you relate the services to a specific department?
- The purchasing group can be helpful
  - Find the company behind the domain
  - Are we purchasing services from them?

Check destination IP address

- Start simple
  - Who manages ASN?
  - Geolocation info?
  - IP delegation
  - PTR records
- Do you recognize the target organization?
  - Business partner or field office
  - Current vendor (active status)
- Other internal IP's connecting?

Some helpful links

https://www.abuseipdb.com/check/<IP Address>

https://otx.alienvault.com/indicator/ip/<IP Address>

https://search.censys.io/hosts/<IP Address>

https://dns.google/query?name=<IP Address>

https://www.google.com/search?q=<IP Address>

https://www.onyphe.io/search/?query=<IP Address>

https://securitytrails.com/list/ip/<IP Address>

https://www.shodan.io/host/<IP Address>

https://www.virustotal.com/gui/ip-address/<IP Address>/relations

C2 Detection Techniques Part 2

What next?

- You've identified connection persistence
- You can't identify a business need
- Next steps
  - Protocol analysis
  - Reputation check of external target
  - Investigate internal IP address

Unexpected app or port usage

- There should be a business need for all outbound protocols
- Research non-standard or unknown ports
  - TCP/5222 (Chrome remote desktop)
  - TCP/5800 & 590X (VNC)
  - TCP/502 (Modbus)
- TeamViewer, AnyDesk, GoToMyPC

Unknown app on standard port

- C2 wants to tunnel out of environment
  - Pick a port likely to be permitted outbound
  - Does not always worry about protocol compliance
- Check standard ports for unexpected apps
  - Indication of tunneling
  - TCP/80 and TCP/443 most common
- Different than app on non-standard port
  - This is sometimes done as "a feature"
  - Example: SSH listening on TCP/2222

Zeek decodes many apps

- Detect over 55 applications
  - HTTP, DNS, SIP, MYSQL, RDP, NTLM, etc. etc.
- Fairly easy to add new ones
  - Example: HL7 if you are in healthcare
- Checks all analyzers for each port
- Does not assume WKP = application

Zeek example

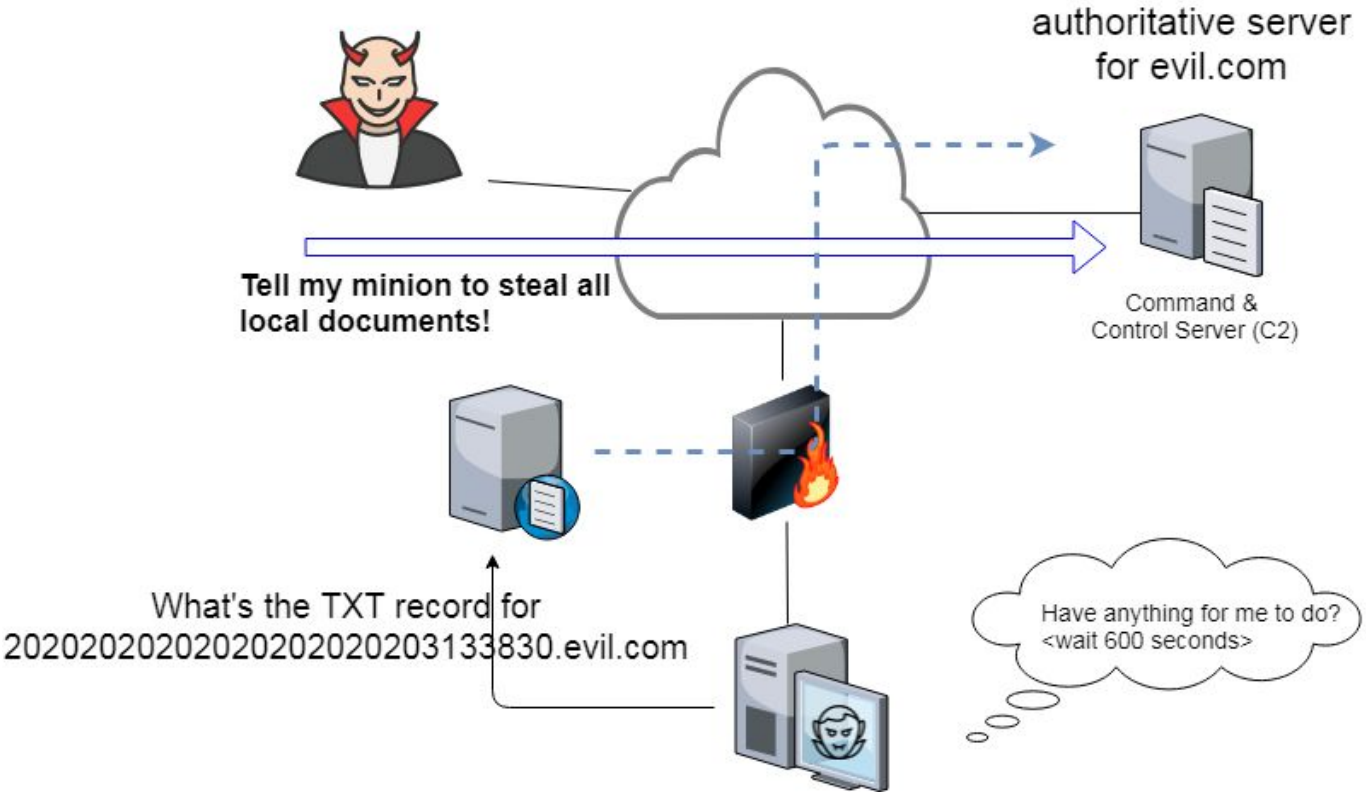
```
thunt@thunt-labs:~/lab1$ cat conn.log | zeek-cut id.orig_h id.resp_h id.resp_p
 proto service orig_ip_bytes resp_ip_bytes | column -t | head
192.168.99.51               104.248.234.238  80    tcp   http  689         403
192.168.99.51               23.223.200.136   80    tcp   -     80          40
192.168.99.51               104.248.234.238  80    tcp   http  729         443
192.168.99.52               224.0.0.251      5353  udp   dns   344         0
fe80::d048:42e0:8448:187c   ff02::fb         5353  udp   dns   424         0
fe80::d048:42e0:8448:187c   ff02::1:3        5355  udp   dns   81          0
192.168.99.52               224.0.0.252      5355  udp   dns   61          0
fe80::d048:42e0:8448:187c   ff02::1:3        5355  udp   dns   81          0
192.168.99.52               224.0.0.252      5355  udp   dns   61          0
192.168.99.51               104.248.234.238  80    tcp   http  689         403
thunt@thunt-labs:~/lab1$
```

AC-Hunter example

Unexpected protocol use

- Attackers may bend but not break rules
- This can result in:
  - Full protocol compliance
  - Abnormal behaviour
- Need to understand "normal"
  - For the protocol
  - For your environment

C2 over DNS


authoritative server
for evil.com
Tell my minion to steal all
local documents!
Command &
Control Server (C2)
What's the TXT record for
20202020202020202020203133830.evil.com
Have anything for me to do?
<wait 600 seconds>

Example: Too many FQDNs

- How many FQDNs do domains expose?
  - Most is < 10
  - Recognizable Internet based vendors 200 - 600
    - Microsoft
    - Akamai
    - Google
    - Amazon
- Greater than 1,000 is suspicious
- Could be an indication of C2 traffic

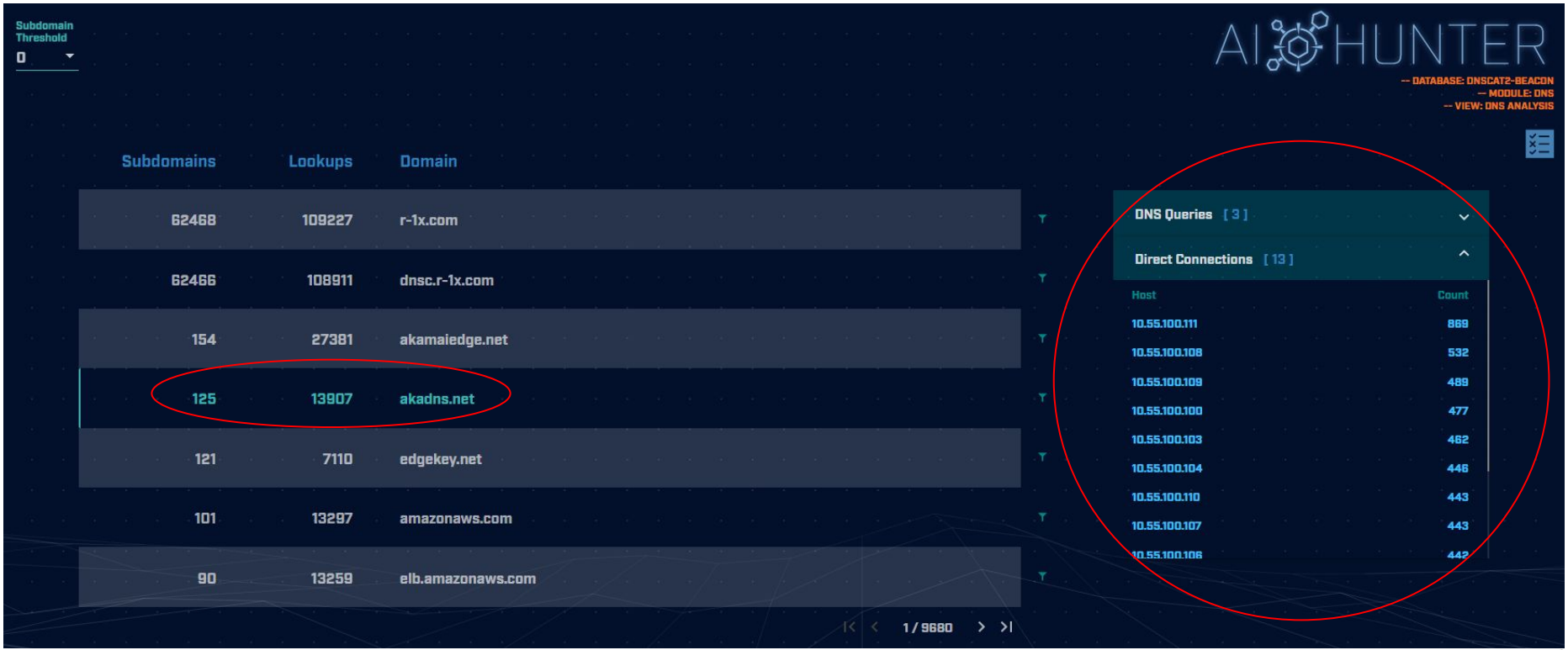
Detecting C2 over DNS

	FQDNs Count	Lookups	Domain
⚠	62468	109227	r-1x.com
⚠	62466	108911	dnsc.r-1x.com
	154	27381	akamaiedge.net
	125	13907	akadns.net

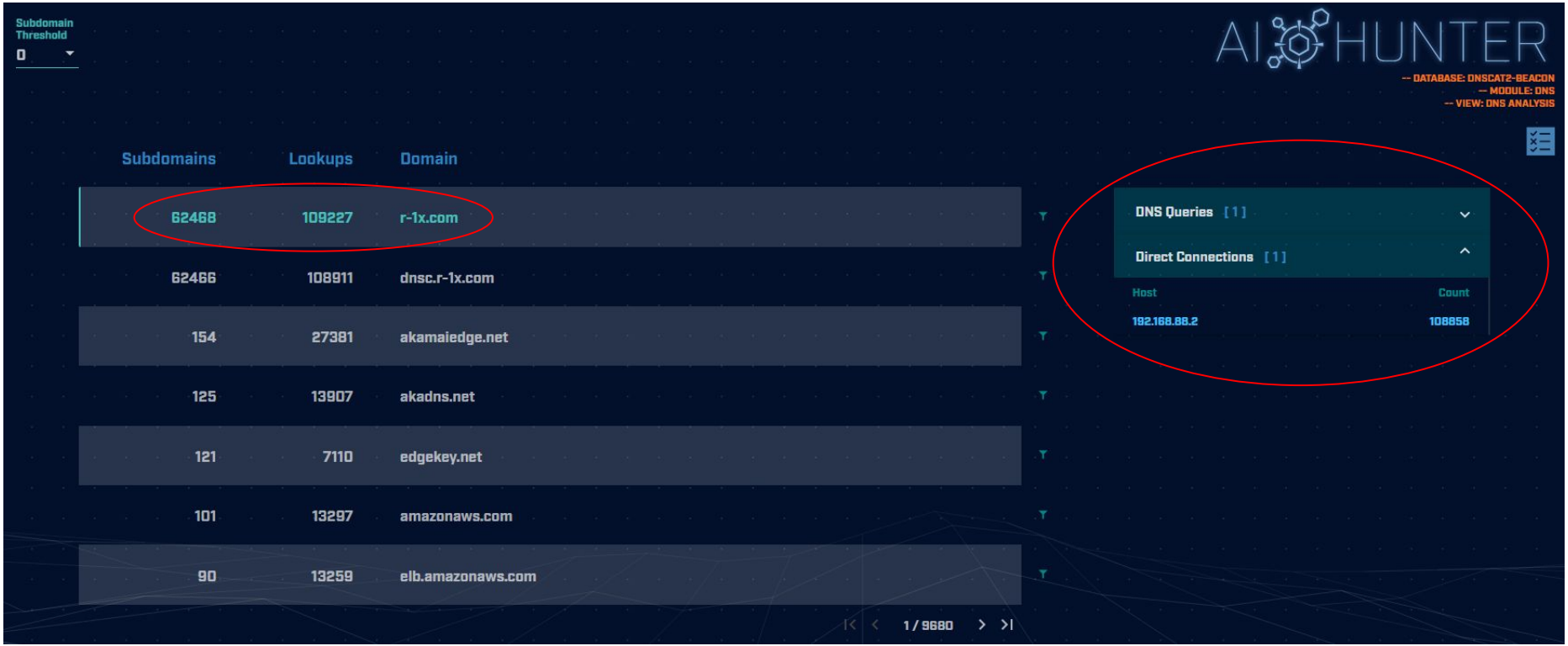
Bonus checks on DNS

- Check domains with a lot of FQDNs
- Get a list of the IPs returned
- Compare against traffic patterns
  - Are internal hosts visiting this domain?
  - Is it just your name servers?
- Unique trait of C2 over DNS
  - Lots or FQDN queries
  - But no one ever connects to these systems

Normal DNS query patten



Things that make you go "hummm"



Look for odd HTTP user agents

```
ritabeakerlab@ritabeakerlab:~/lab1$ cat http.log | zeek-cut id.orig_h id.resp_h user_agent
 | grep 10.0.2.15 | sort | uniq | cut -f 3 | sort | uniq -c | sort -rn
     15 Microsoft-CryptoAPI/10.0
     12 Microsoft-WNS/10.0
      1 Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 5.2) Java/1.5.0_08
ritabeakerlab@ritabeakerlab:~/lab1$
```

10.0.2.15 identifies itself as:

Windows 10 when speaking to 27 different IP's on the Internet
Windows XP when speaking to one specific IP on the Internet

Unique SSL Client Hello: Zeek + JA3

SSL/TLS Hash	Seen	Requests	Sources
5e573c9c9f8ba720ef9b18e9fce2e2f7	1	clientservices.googleapis.com	10.55.182.100
bc6c386f480ee97b9d9e52d472b772d8	2	clients4.google.com, 556-emw-319.mktoresp.com	10.55.182.100
f3405aa9ca597089a55cf8c62754de84	2	builds.cdn.getgo.com	10.55.182.100
28a2c9bd18a11de089ef85a160da29e4	2	mediaredirect.microsoft.com	10.55.100.105, 10.55.182.100
08bf94d7f3200a537b5e3b76b06e02a2	4	files01.netgate.com	192.168.88.2

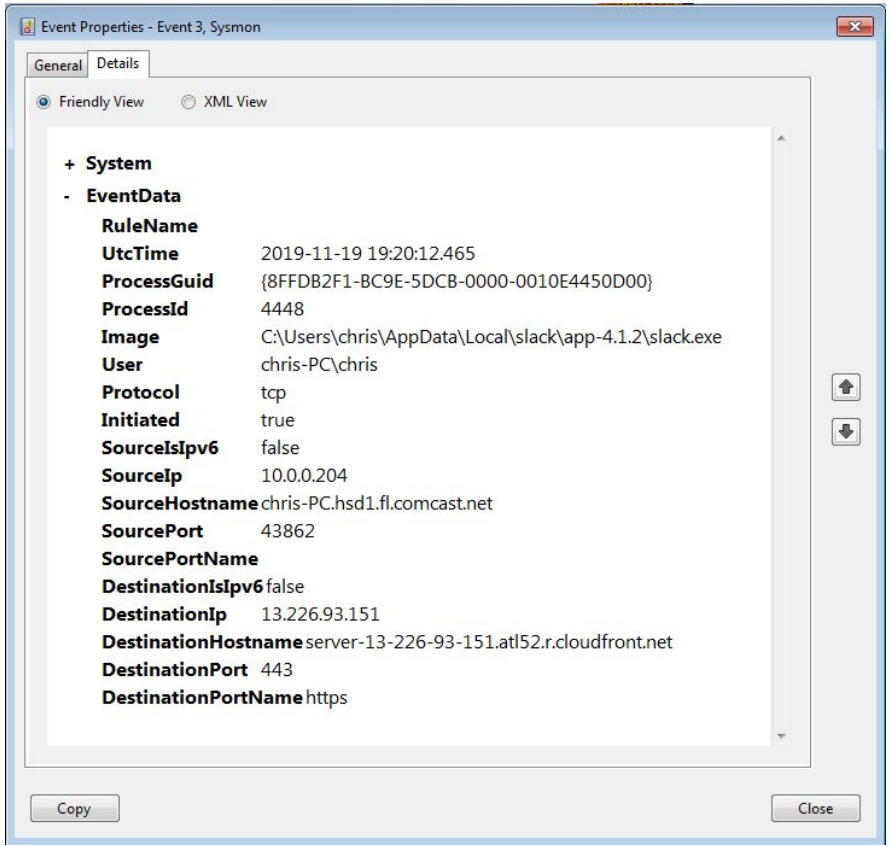
Internal system

- Info available varies greatly between orgs
- Inventory management systems
- Security tools like Carbon Black
- OS projects like BeaKer
- Internal security scans
- DHCP logs
- Login events
- Passive fingerprinting

Leverage internal host logging

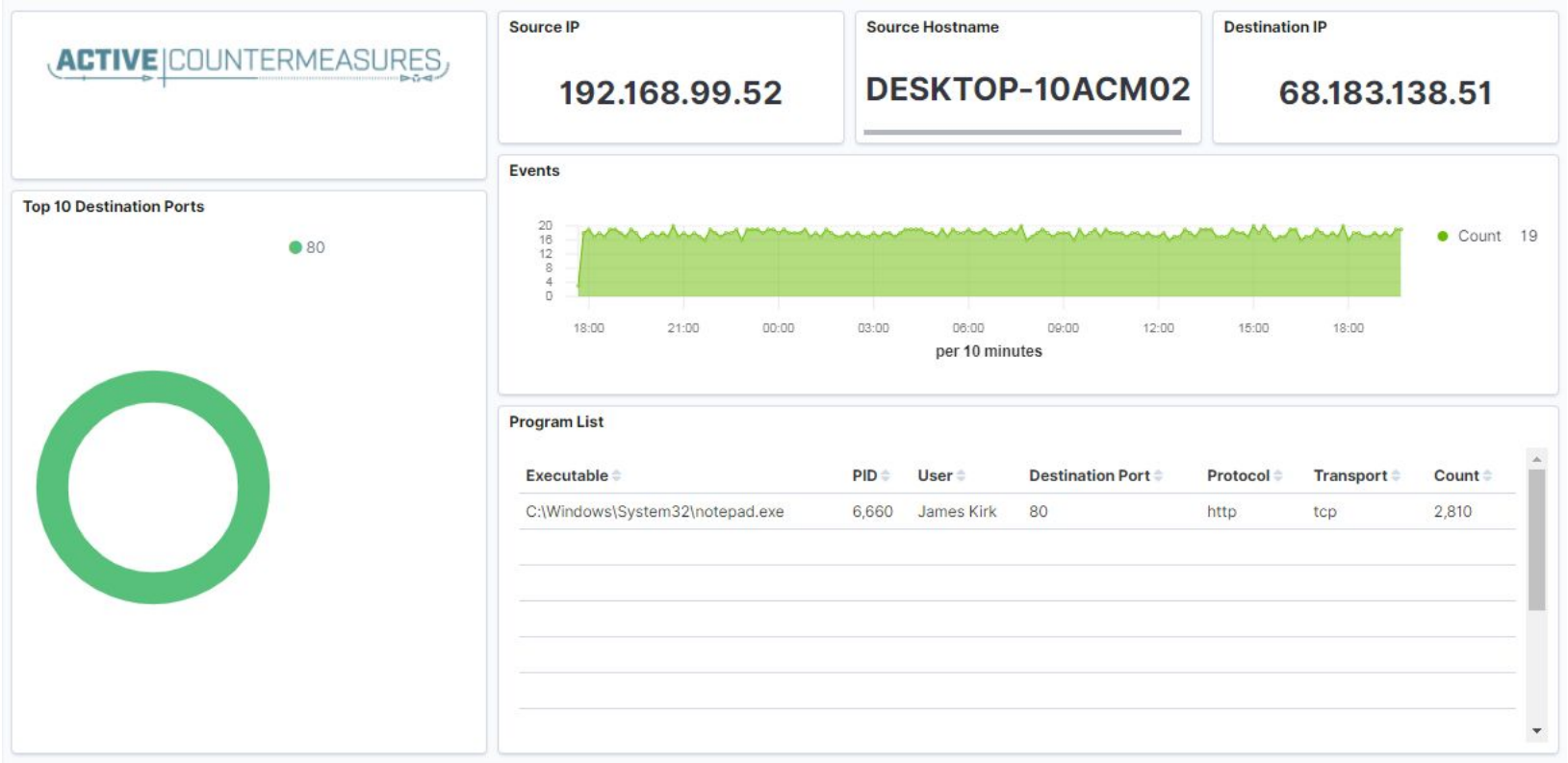
- Network shows suspicious traffic patterns
- Use this data to pivot to host logs
- Filter your logs based on:
  - Suspect internal host
  - Timeframe being analyzed
- Anything stand out as unique or odd?

Sysmon Event ID Type 3's



Map outbound connections to the applications that created them.

Sysmon Type 3 + BeaKer



But I have no system logs!

- Good time to start collecting them
- Full packet captures from system
- Apply additional network tools to collect more data
- Just remember, no detectable actions until we trigger incident response mode!

What next?

- Disposition session
  - "I think it's safe" = add to safelist
  - "I think we've detected a compromise" = Incident response mode
- Remember to leave no footprints
  - All actions undetectable to potential adversaries
  - Passive activities only
- Incident response may include active tasks

Network Threat Hunting Tools

capinfos

- Print summary info regarding pcaps
- For a decent hunt you want 12+ hours
- 86,400 seconds = 24 hours

```
cbrenton@guess:~/c2$ capinfos -aeu evilosx_24hr.pcap
File name:           evilosx_24hr.pcap
Capture duration:    86291.558021 seconds
First packet time:   2021-02-17 03:40:26.100491
Last packet time:    2021-02-18 03:38:37.658512
cbrenton@guess:~/c2$
```

tcpdump

- What's it good for?
  - Lightweight packet capturing tool
  - Cross platform support (windump on Windows)
- When to use it
  - Audit trail of all traffic
  - Can also filter to see only specific traffic
  - Can be fully automated
- Where to get it

https://www.tcpdump.org/

tcpdump example

- Debian/Ubuntu
  - Place the following in /etc/rc.local
- Red Hat/CentOS, Fedora
  - Place the following in /etc/rc.d/rc.local
- Grabs all traffic and rotates every 60 min
  - Date/time stamped and compressed

```
#Place _above_ any "exit" line
mkdir -p /opt/pcaps
screen -S capture -t capture -d -m bash -c "tcpdump -ieth0 -G
3600 -w '/opt/pcaps/`hostname -s`.%Y%m%d%H%M%S.pcap' -z bzip2"
```

tshark

- What's it good for?
  - Extracting interesting fields from packet captures
  - Multiple passes to focus on different attributes
  - Combine with text manipulation tools
  - Can be automated
- When to use it
  - Both major and minor attributes
- Where to get it

https://www.wireshark.org/

Tshark example - DNS queries

```
$ tshark -r thunt-lab.pcapng -T fields -e dns.qry.name
udp.port==53 | head -10

6dde0175375169c68f.dnsc.r-1x.com
6dde0175375169c68f.dnsc.r-1x.com
0b320175375169c68f.dnsc.r-1x.com
0b320175375169c68f.dnsc.r-1x.com
344b0175375169c68f.dnsc.r-1x.com
344b0175375169c68f.dnsc.r-1x.com
0f370175375169c68f.dnsc.r-1x.com
0f370175375169c68f.dnsc.r-1x.com
251e0175375169c68f.dnsc.r-1x.com
251e0175375169c68f.dnsc.r-1x.com
```

Tshark example - user agents

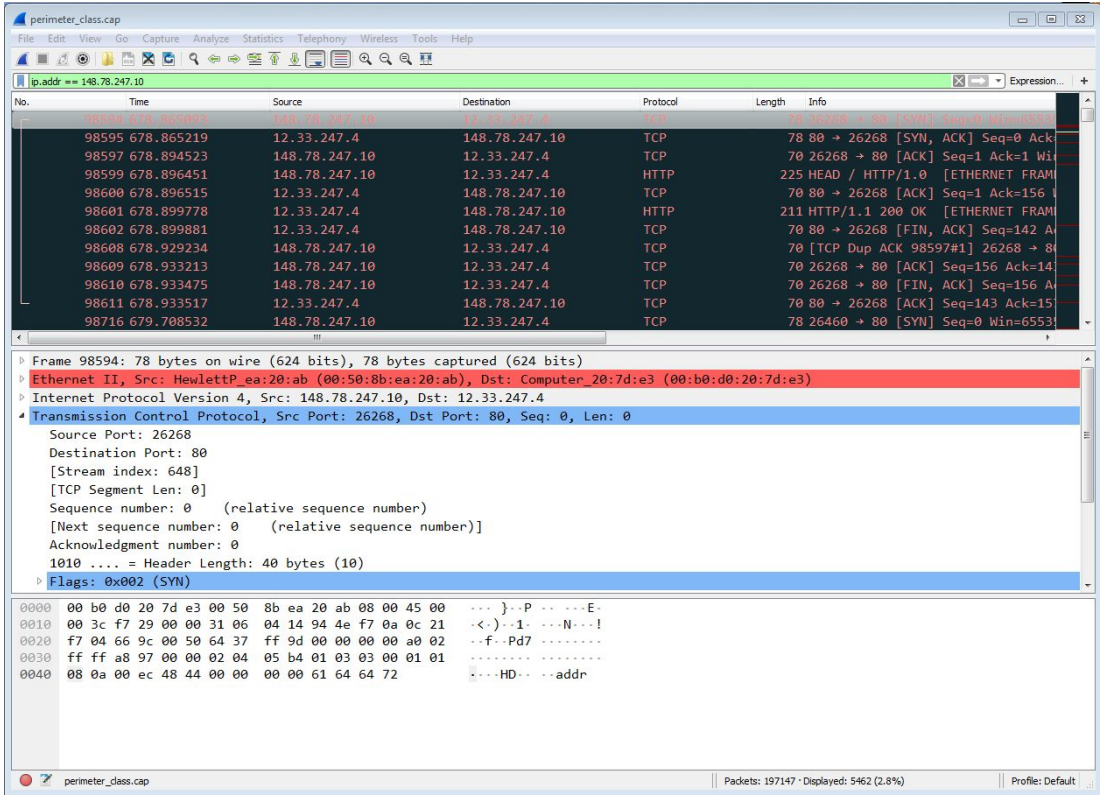
```
$ tshark -r sample.pcap -T fields -e http.user_agent tcp.
dstport==80 | sort | uniq -c | sort -n | head -10
      2 Microsoft Office/16.0
      2 Valve/Steam HTTP Client 1.0 (client;windows;10;1551832902)
      3 Valve/Steam HTTP Client 1.0
     11 Microsoft BITS/7.5
     11 Windows-Update-Agent
     12 Microsoft-CryptoAPI/6.1
    104 PCU
```

Wireshark

- What's it good for?
  - Packet analysis with guardrails
  - Stream level summaries
- When to use it
  - As part of a manual analysis
  - When steps cannot be automated
- Where to get it

https://www.wireshark.org/

Useful when I have a target



Zeek

- Network recorder
- What's it good for?
  - Near real time analysis (1+ hour latency)
  - More storage friendly than pcaps
- When to use it
  - When you need to scale
  - When you know what attributes to review
- Where to get it

https://www.zeek.org/
sudo apt -y install zeek

Zeek example - cert check

```
$ cat ssl* | zeek-cut id.orig_h id.resp_h id.resp_p
validation_status | grep 'self signed' | sort | uniq
122.228.10.51   192.168.88.2    9943    self signed certificate in
certificate chain
24.111.1.134    192.168.88.2    9943    self signed certificate in
certificate chain
71.6.167.142    192.168.88.2    9943    self signed certificate in
certificate chain
```

-d for human readable times

- Zeek-cut prints epoch time by default
- "-d" converts to human readable

```
cbrenton@cbrenton-beacon-src-test:~/foo$ cat conn.01\:00\:00-02\
:00\:00.log | zeek-cut ts id.orig_h | head -8
1645578000.318671       167.172.154.151
1645578000.318784       167.172.154.151
1645578000.318841       167.172.154.151
1645578000.334906       167.172.154.151
1645578000.334948       167.172.154.151
1645578000.334977       167.172.154.151
1645578001.228742       167.172.154.151
1645578001.360749       167.172.154.151
cbrenton@cbrenton-beacon-src-test:~/foo$ cat conn.01\:00\:00-02\
:00\:00.log | zeek-cut -d ts id.orig_h | head -8
2022-02-23T01:00:00+0000        167.172.154.151
2022-02-23T01:00:00+0000        167.172.154.151
2022-02-23T01:00:00+0000        167.172.154.151
2022-02-23T01:00:00+0000        167.172.154.151
2022-02-23T01:00:00+0000        167.172.154.151
2022-02-23T01:00:00+0000        167.172.154.151
2022-02-23T01:00:01+0000        167.172.154.151
2022-02-23T01:00:01+0000        167.172.154.151
cbrenton@cbrenton-beacon-src-test:~/foo$
```

zcutter.py

- zeek-cut limited to CSV format
- What if you use JSON?
- zcutter.py to the rescue!
- Like zeek-cut, but supports CSV & JSON
- Will also process multiple log files simultaneously

https://raw.githubusercontent.com/activecm/zcutter/main/zcutter.py

Passer

```
TC,172.1.199.23,TCP_43,open,
TC,172.16.199.23,TCP_55443,open,
UC,172.16.199.23,UDP_626,open,serialnumberd/clientscanner likely nmap
scan Warnings:scan
UC,172.16.199.23,UDP_1194,open,openvpn/client Warnings:tunnel
UC,172.16.199.23,UDP_3386,open,udp3386/client
UC,172.16.199.23,UDP_5632,open,pcanywherestat/clientscanner
Warnings:scan
UC,172.16.199.23,UDP_64738,open,shodan_host/clientscanner abcdefgh
Unlisted host Warnings:scan
DN,2001:db8:1001:0000:0000:0000:0000:0015,AAAA,ns3.markmonitor.com.,
DN,fe80:0000:0000:0000:189f:545b:7d4c:eeb8,PTR,Apple
TV._device-info._tcp.local.,model=J105aA
```

Smudge

```
.-[ 192.168.99.51/52864 -> 104.248.234.238/80 ]-
|
| client = 192.168.99.51/52864
| os = Windows 7
| certainty = 40%
| dist = 0
| raw_sig = 4:128:0:1460:65535:8:M1460,N,W8,N,N,S:df,id+,ack-,uptr+:0
|
`----
```

Can run it alone or integrated with Passer

ngrep

- Pattern match on passing packets
- Like "grep" for network traffic
- Useful for quick checks
  - NIDS with signature better choice for long term
- Useful switches
  - "-q" = Don't print "#" for non-matches
  - "-I" = Read a pcap file

https://github.com/jpr5/ngrep
sudo apt install ngrep

ngrep example

```
cbrenton@cbrenton-lab-testing:~/pcaps$ ngrep -q -I odd.pcap Admin | head -15
input: odd.pcap
match: Admin

T 148.78.247.10:26922 -> 12.33.247.4:80 [AP]
  GET /cfide/Administrator/startstop.html HTTP/1.0..Host: 12.33.247.4..User-Agent: Mozilla/5.0 [en] (Win
  95; U)..Referer: http://12.33.247.4/..X-Forwarded-For: 148.64.147.168..Cache-Control: max-stale=0..Pra
  gma: no-cache......Cv

T 12.33.247.4:80 -> 148.78.247.10:26922 [AP]
  HTTP/1.1 404 Not Found..Date: Tue, 25 Jun 2002 00:34:58 GMT..Server: Apache..Connection: close..Conten
  t-Type: text/html; charset=iso-8859-1....<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<HTML><HEA
  D>.<TITLE>404 Not Found</TITLE>.</HEAD><BODY>.<H1>Not Found</H1>.The requested URL /cfide/Administrato
  r/startstop.html was not found on this server.<P>.</BODY></HTML>.....

T 12.33.247.4:80 -> 148.78.247.10:26922 [AFP]
cbrenton@cbrenton-lab-testing:~/pcaps$ _
```

RITA

- What's it good for?
  - Beacon & long conn at scale
  - Some secondary attributes
- When to use it
  - Can better organize Zeek data
  - Good when you are comfortable scripting
  - Will scale but can be time consuming
- Where to get it

https://github.com/activecm/rita

RITA example - beacons

```
cbrenton@cb-lab:~/lab1$ rita show-beacons lab1 | head
Score,Source IP,Destination IP,Connections,Avg. Bytes,Intvl Range,Size Range,Top
Intvl,Top Size,Top Intvl Count,Top Size Count,Intvl Skew,Size Skew,Intvl Dispersi
on,Size Dispersion,Total Bytes
1,10.55.100.111,165.227.216.194,20054,92,29,52,1,52,7774,20053,0,0,0,0,1845020
0.838,10.55.200.10,205.251.194.64,210,308,29398,4,300,70,109,205,0,0,0,0,64850
0.835,10.55.200.11,205.251.197.77,69,308,1197,4,300,70,38,68,0,0,0,0,21313
0.834,10.55.100.111,34.239.169.214,34,1259,5,14388,1,156,15,30,0,0,0,0,42831
0.834,192.168.88.2,13.107.5.2,27,198,2,33,12601,73,4,15,0,0,0,0,5370
0.833,10.55.100.107,23.52.161.212,24,5404,43235,52,1800,505,19,21,0,0,0,0,129717
0.833,10.55.100.107,23.52.162.184,24,2397,43356,52,1800,467,18,18,0,0,0,0,57540
0.833,10.55.100.111,23.52.161.212,27,5379,37752,92,1800,505,17,20,0,0,0,0,145256
0.833,10.55.100.109,23.52.161.212,26,5417,39646,52,1800,505,21,20,0,0,0,0,140848
cbrenton@cb-lab:~/lab1$ _
```

Scale is 0 - 1 with 1.0 being a perfect beacon score

RITA can also check

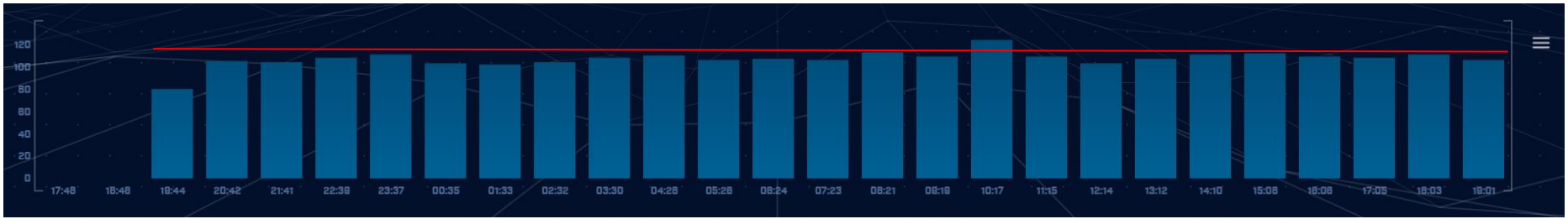
- Beacons based on HTTP/host or TLS/SNI
- Beacons based on FQDN
- Beacons through SOCKS server
- Long connections
- Still open (not yet logged) connections
- C2 over DNS
- Matches against your threat intel list

AC-Hunter (Community & Enterprise)

Score ranking on the left, breakdown of scores on the right

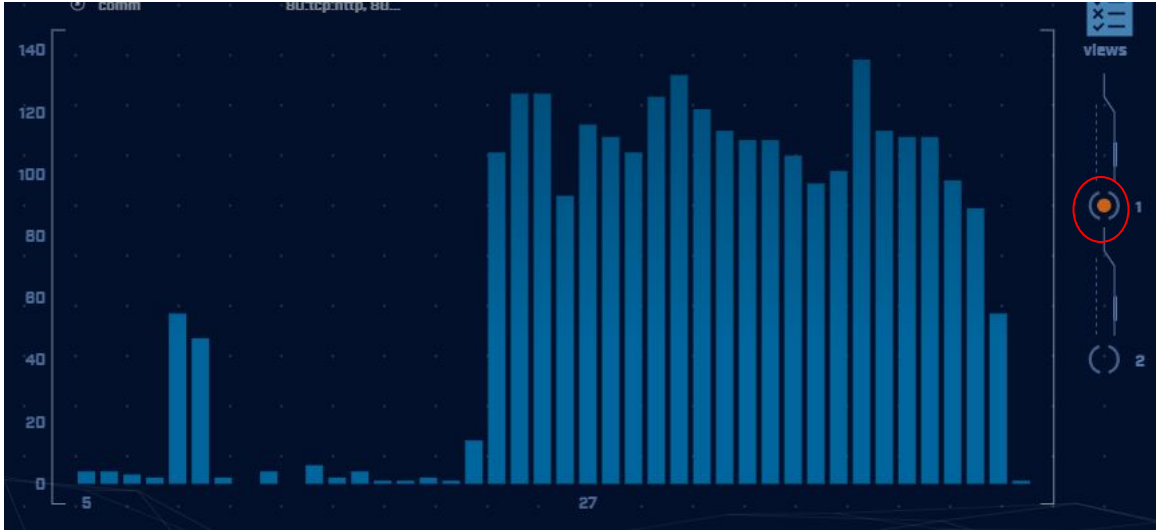
Beacon screen

Beacon analysis - 24 hour graph



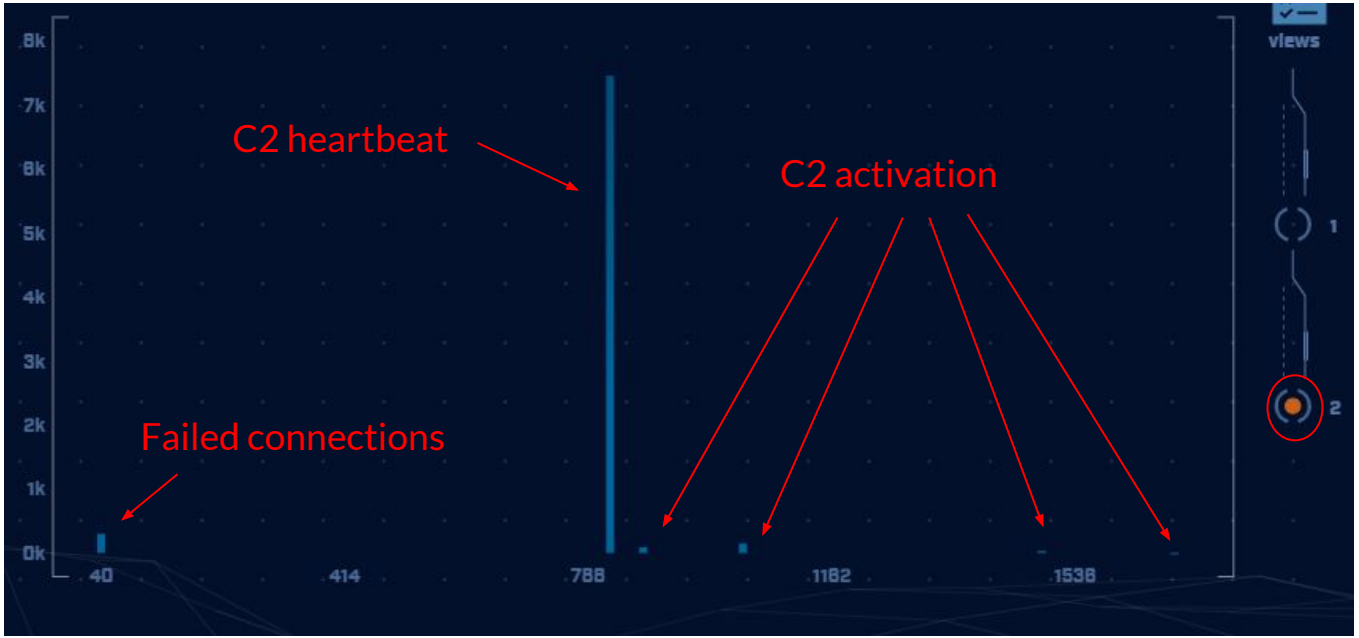
Multiple hours showing the same number of connections

Time interval count



Frequency of a specific time delta between connections
Varied timing like this indicates jitter

View 2 = Session size analysis



Target investigation

Click IP to open Web investigation options

Click to add to safelist

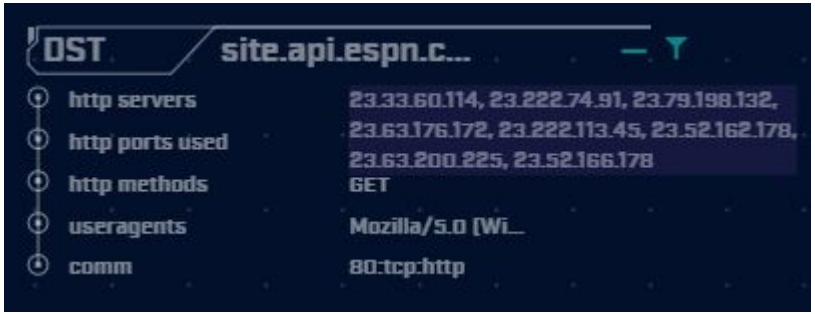
Generic location info

What did the user query via DNS before connecting to this IP address?

Protocol data

Beacon Web analysis

Default display



Mouse over first HTTP server's IP address
C2 connecting to multiple IPs via CDN

ACH - Long connections

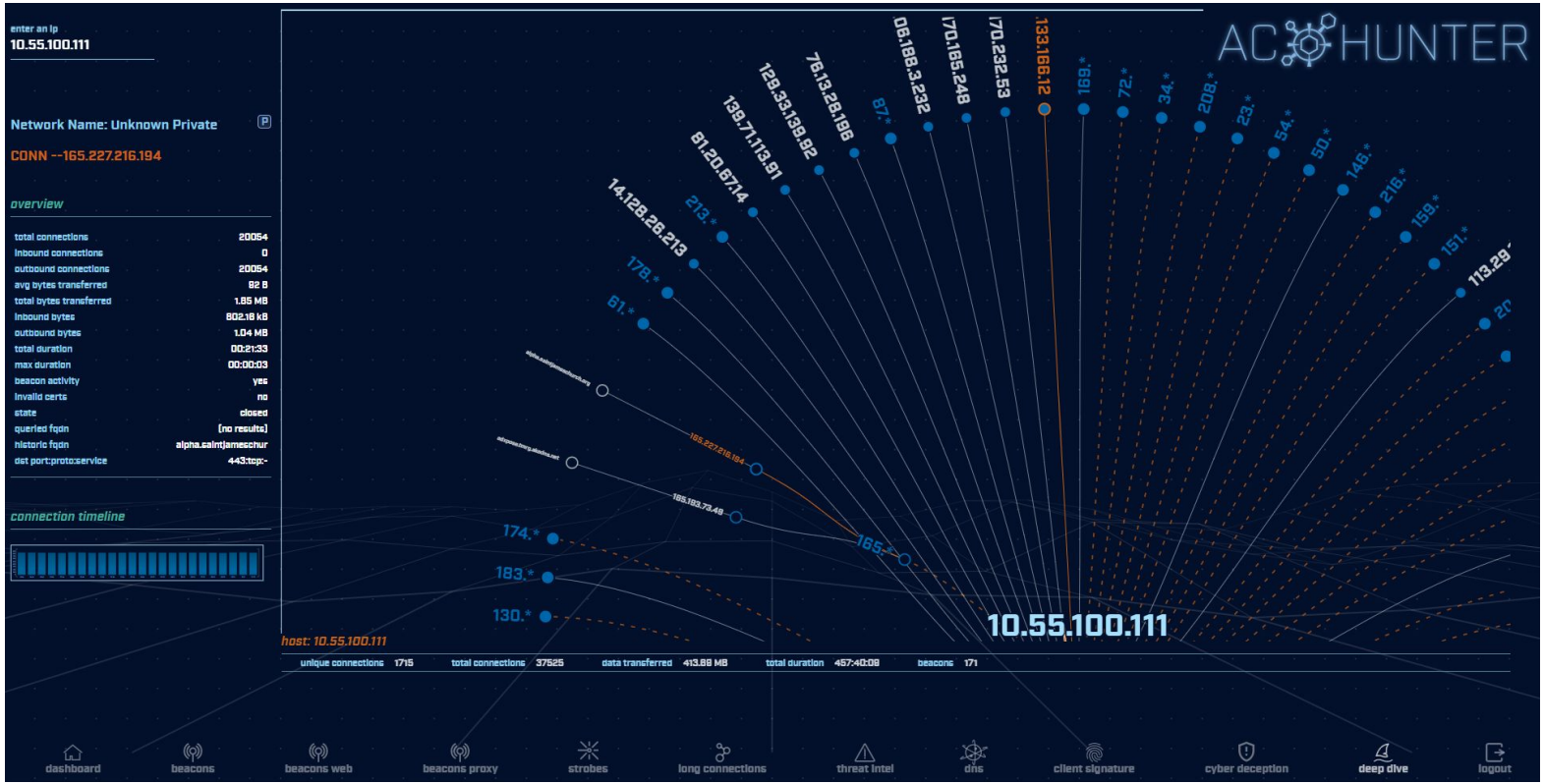
ACH - Threat intel

- Score 10 points when a match is identified
- Monitor bytes from internal to external
- If > 5 MB, start adding in more points
- If >= 25 MB, increase score by 100 points

ACH - Cyber deception

Use canary tokens to create tripwires within your environment

ACH - Deep dive

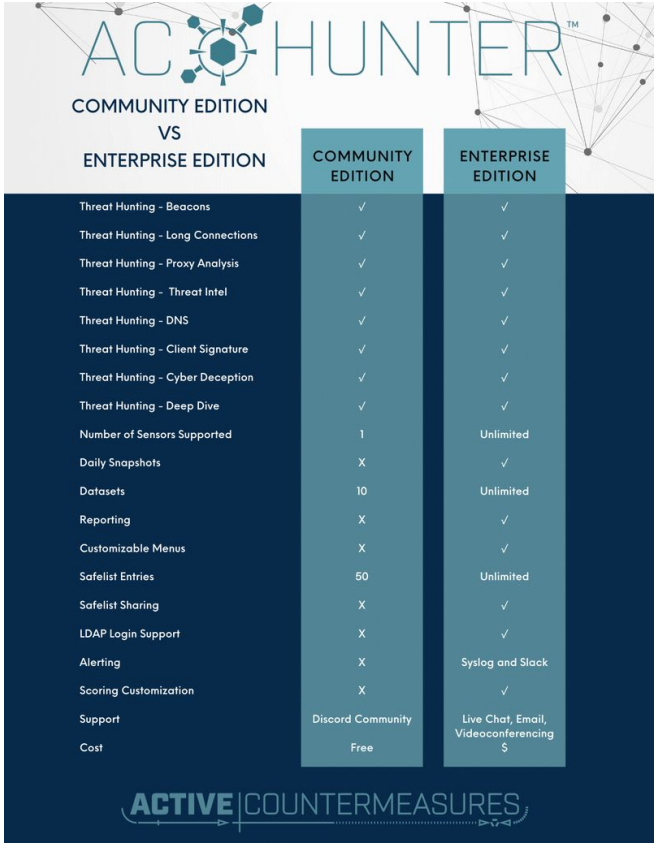


Install process

```
threat@ACH:~/Downloads/achunter$ ./install_acm.sh

================ Selecting Installation Components ================
Do you wish to install AC-Hunter (Y/N)? y
What is the hostname or IP address of the system on which to install AC-Hunter (enter    127.0.0
.1    if you wish to install it on this system)
127.0.0.1
Do you wish to install Zeek (Y/N)? y
What is the hostname or IP address of the system on which to install Zeek (enter    127.0.0.1
 if you wish to install it on this system)
127.0.0.1
Do you wish to install Active-Flow (Y/N)? n
Do you wish to install Beaker (Y/N)? _
```

Options:
Install from binary (above) - More time, smaller download, most flexibility
Download official VM - Pretty much ready to go with minor tweaking, larger download
VM for this class - Labs to guide learning, largest download

CE Versus Enterprise



Internal DNS zone transfers

- Internal host names can be more useful than IPs
- Especially in DHCP environments
- Help sync data with host based tools
- Data can be collected via regular zone transfers
  - Should sync with DHCP lease time
  - Once per hour or more usually sufficient
- Working on integrating this feature into RITA and AC-Hunter

Datamash

- What's it good for?
  - Similar to the R-base tools, but more extensive
  - Performing simple calculation on data
- When to use it
  - Performing calculations on multiple lines
  - Statistical analysis
- Where to get it

https://www.gnu.org/software/datamash/
sudo apt install datamash

Datamash

- Used for processing raw data at the command line
- Great for sifting through tabulated data
  - Like Zeek logs
- Can perform statistical analysis
  - Min, max, mean, etc.
  - Can add together values

Datamash example

```
cbrenton@cbrenton-lab-testing:~/lab3$ cat conn.log | zeek-cut
id.orig_h id.resp_h duration | sort -k3 -rn | head -5
192.168.1.105   143.166.11.10   328.754946
192.168.1.104   63.245.221.11   41.884228
192.168.1.104   63.245.221.11   31.428539
192.168.1.105   143.166.11.10   27.606923
192.168.1.102   192.168.1.1     4.190865

cbrenton@cbrenton-lab-testing:~/lab3$ cat conn.log | zeek-cut
id.orig_h id.resp_h duration | grep -v -e '^$' | grep -v '-' | sort |
datamash -g 1,2 sum 3| sort -k3 -rn | head -5
192.168.1.105   143.166.11.10   356.361869
192.168.1.104   63.245.221.11   73.312767
192.168.1.102   192.168.1.1     5.464553
192.168.1.103   192.168.1.1     4.956918
192.168.1.105   192.168.1.1     1.99374
```

Duplicate IPs

Beacon/Threat Simulator

- Permits you to test your C2 detection setup
- Target any TCP or UDP port
- Can jitter timing
- Can jitter payload size
- Not designed to exfiltrate data!

```
beacon-simulator.sh <target IP> 80 300 10 tcp 5000
```

Connect to TCP/80 on target IP every 300 seconds, +/-10 seconds, vary payload between 0-5,000 bytes

https://github.com/activecm/threat-tools

What if I need specific app data?

```
#beacon-test
while :
do
        curl -A 'Modzilla/0.0001 (Atari 7800)' $1 >/dev/null 2>&1
        sleep $(shuf -i200-350 -n1)
done
```

Then run this command with screen:

```
screen -S c2 -d -m /bin/beacon-test <Target IP or FQDN>
```

Packet crafting tools like hping3 let you define payload

Create your own scripts!

```
cbrenton@cb-lab:~/lab1$ cat /bin/fq
echo 'DNS info'
cat dns.* | zeek-cut answers query | sort | uniq | grep -Fw $1
echo 'HTTP info'
cat http.* | zeek-cut id.resp_h host user_agent | sort | uniq | grep -Fw $1
echo 'TLS info'
cat ssl.* | zeek-cut id.resp_h server_name validation_status | sort | uniq | grep -Fw $1
cbrenton@cb-lab:~/lab1$ fq 69.172.216.56
DNS info
anycast.fw.adsafeprotected.com,69.172.216.56    fw.adsafeprotected.com
HTTP info
TLS info
69.172.216.56   fw.adsafeprotected.com  ok
cbrenton@cb-lab:~/lab1$
```

Example script you can create to make life easier
"fq" check dns.log, http.log and ssl.log **in the local directory**
Returns info on specified IP address of FQDN
Use "zcat" if logs are in compressed format

C2 Labs & Walkthroughs

What We Will Cover

- This section is mostly hands on labs
- Implement what you have learned
- Two formats:
  - Guided walkthrough - Just follow along
  - Labs - Try to solve the problem on your own
  - Labs have a "hints" page if you get stuck
- Walkthroughs stress familiarization
- Labs used to cement your knowledge
  - Hints provided if needed

Reminder

- Class VM
  - SSH login - threat
  - SSH pass - hunting
  - Web login - threat@activecountermeasures.com
  - Web pass - hunting2

Guided tour - Finding the lab files

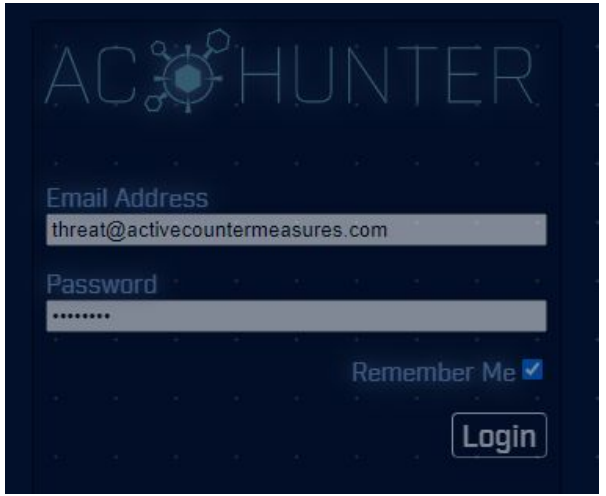
```
threat@ACH:~$ pwd
/home/threat
threat@ACH:~$ ls
Desktop    Downloads  Music     Public  Templates
Documents  labs       Pictures  snap    Videos
threat@ACH:~$ cd labs
threat@ACH:~/labs$ ls
lab1  lab2  lab3
threat@ACH:~/labs$ cd lab1
threat@ACH:~/labs/lab1$ ls
capture_loss.log  http.log            packet_filter.log
certs-remote.pem  known_hosts.log     software.log
conn.log          known_services.log  ssl.log
dhcp.log          loaded_scripts.log  stats.log
dns.log           notice.log          x509.log
files.log         ntp.log
threat@ACH:~/labs/lab1$
```

Guided tour - Login to ACH

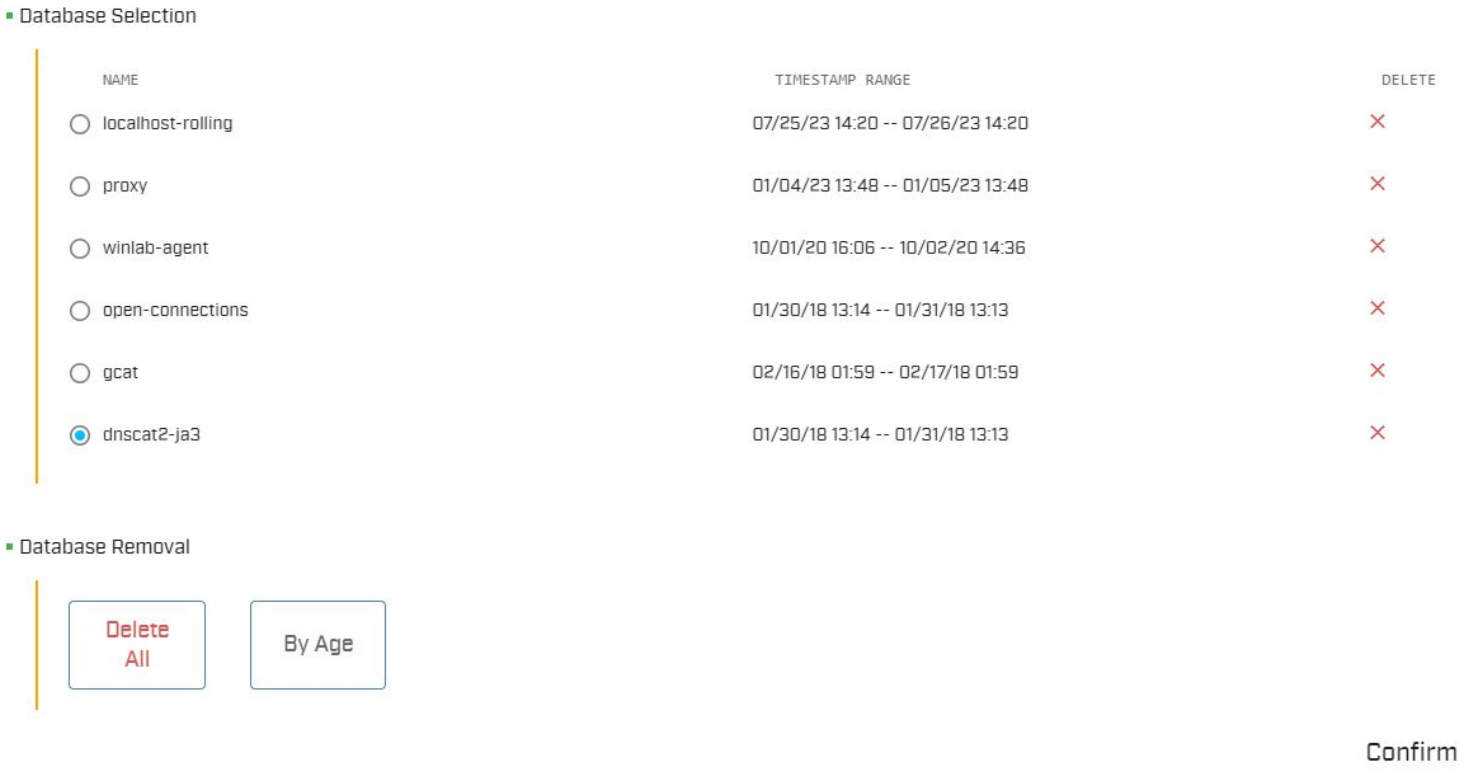
Working from the VM desktop

Working remote from host with VirtualBox

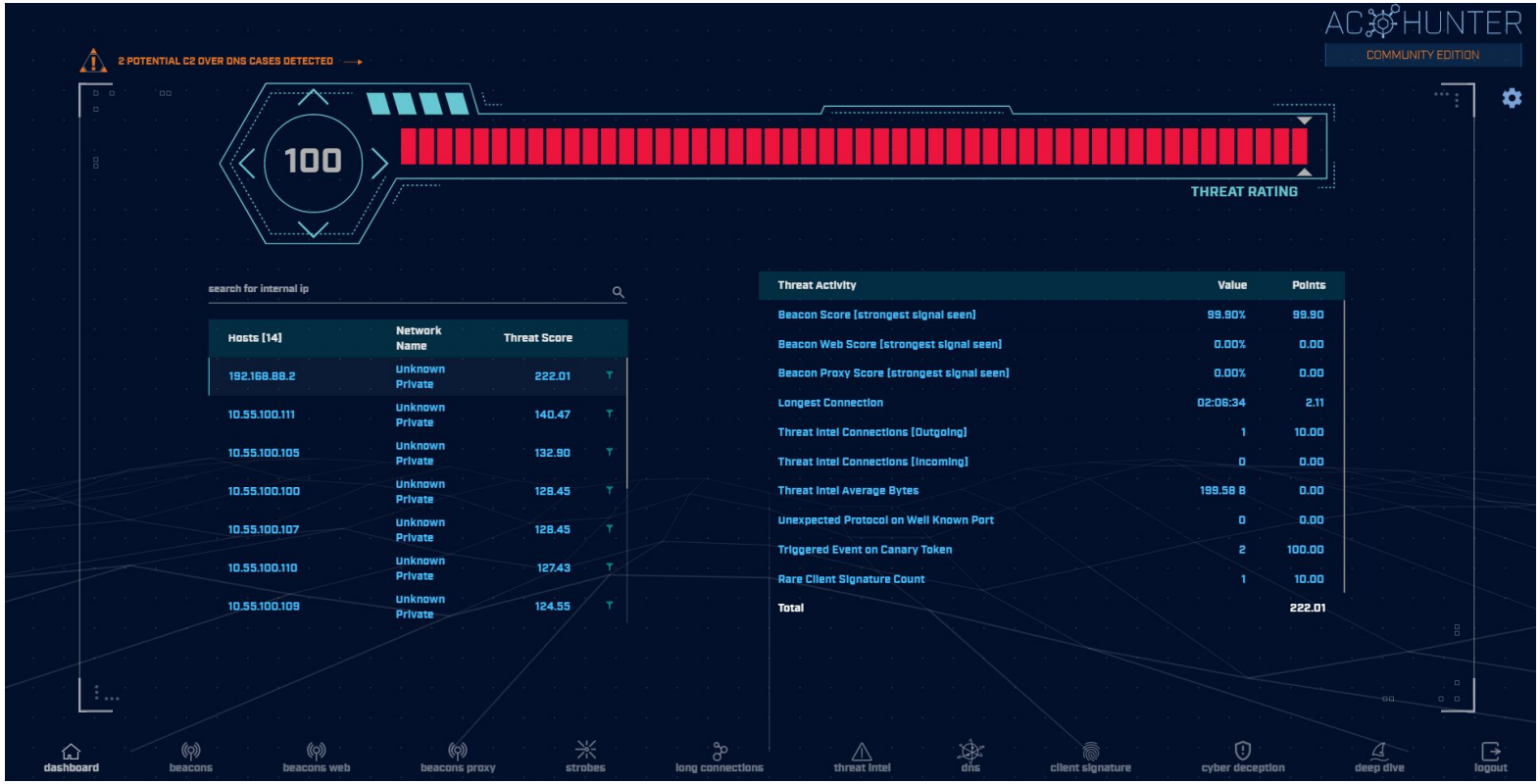
Working remote from host with VMWare



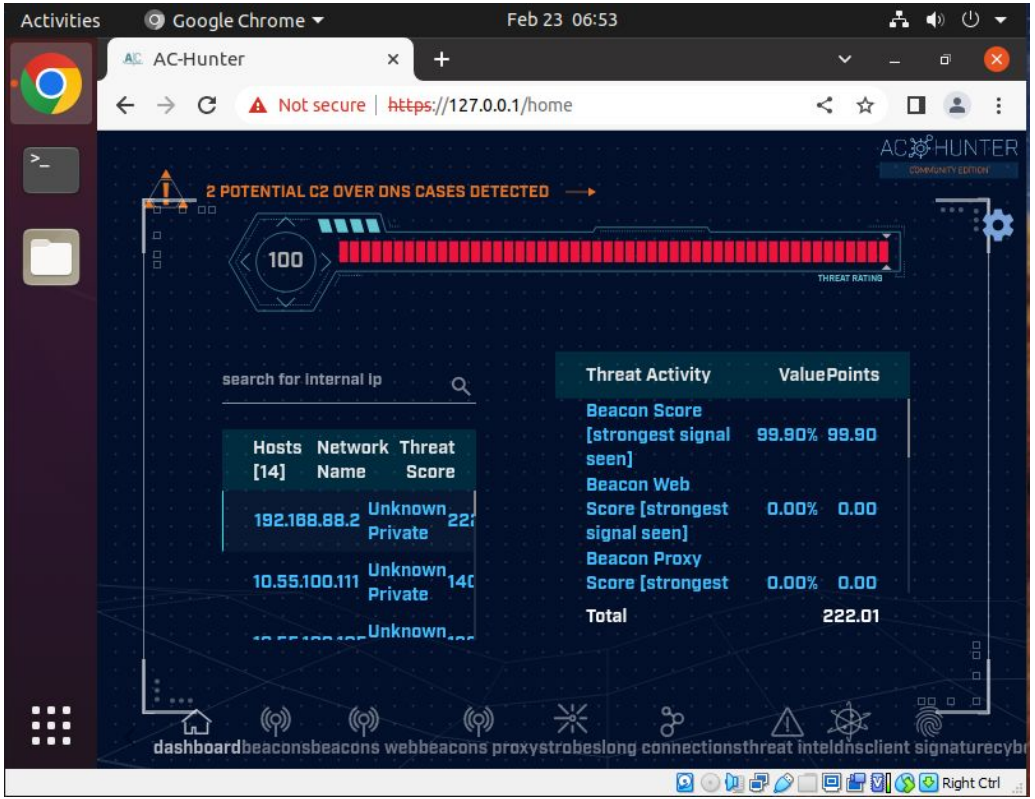
Guided tour - First login



Guided tour - What you should see

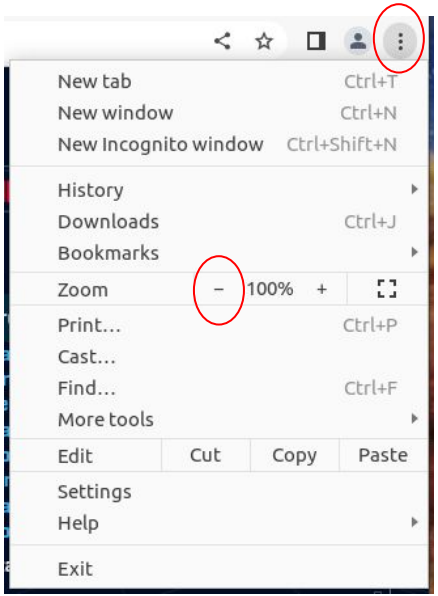


Guided tour - What if I see this?

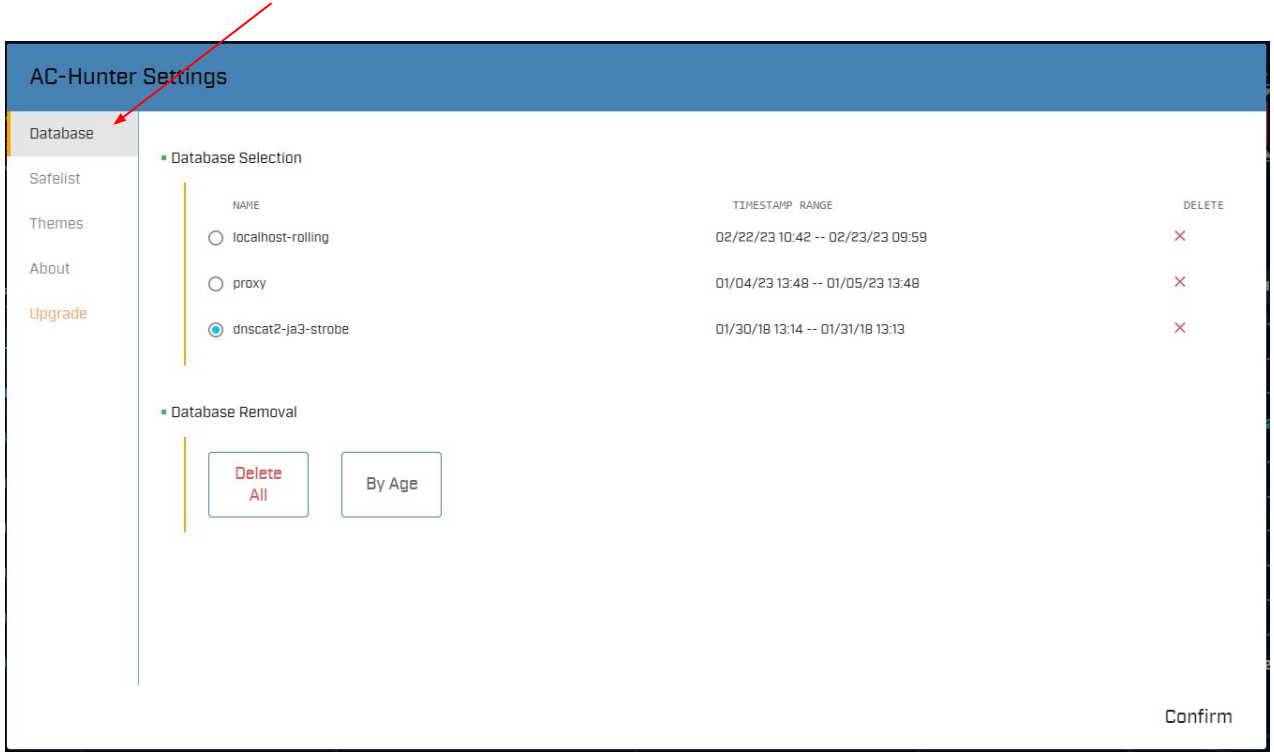


Change VM View to full screen

Zoom out Chrome



Changing databases



Let's add a safelist entry

- Used when legit business need is identified
- Keep the entry from showing up in hunts
- Applied across all databases
- Does not delete data!
  - Hides from view
  - Hides from scoring
- Remove entry and data returns

Guided walkthrough - safelisting

Click "beacons web" on bottom of the dashboard

Select second IP in list

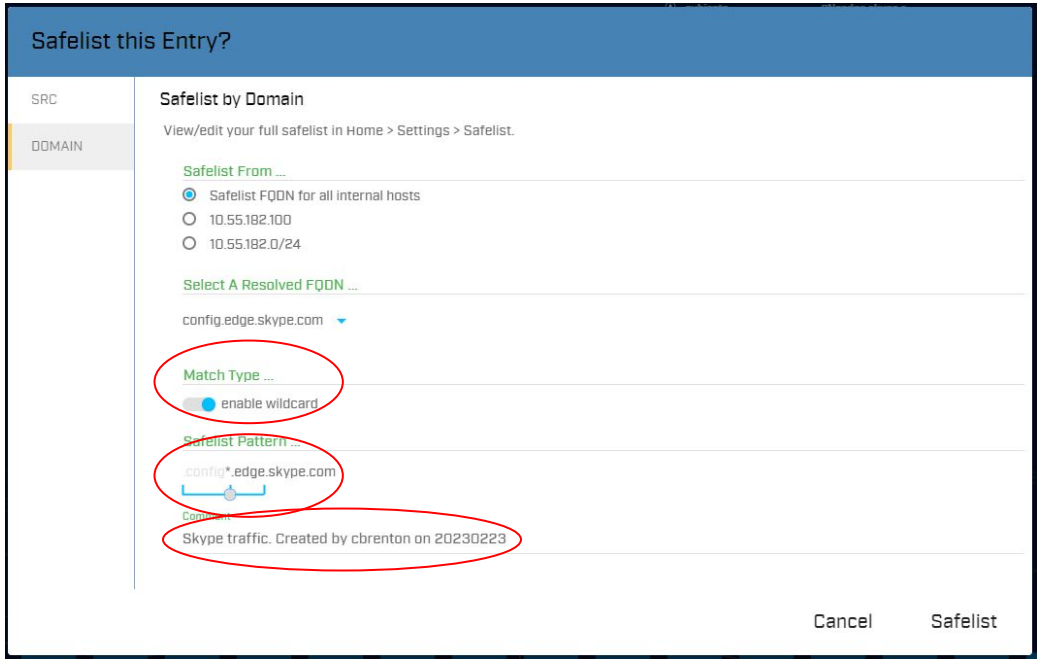
Guided walkthrough - Analyze

Traffic to skype.com with a legitimate digital certificate
Assume Skype is an approved business app

Guided walkthrough - Safelist

Click the filter icon to add this entry to the safelist

Guided walkthrough - Safelist

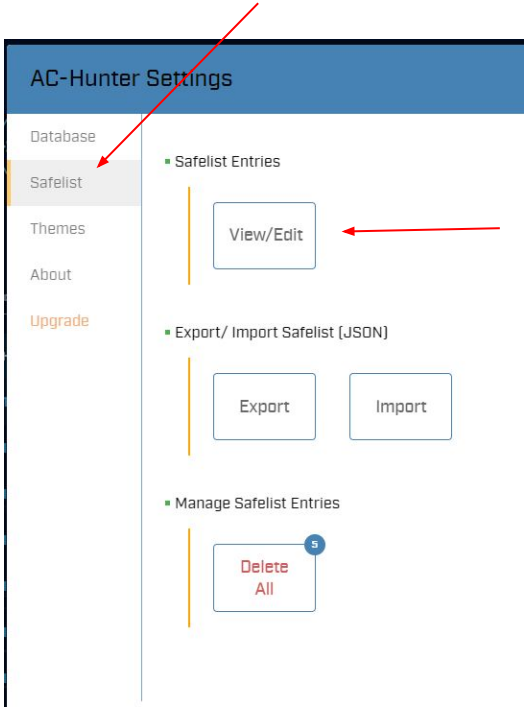


When no FQDN info, implement based on IP
Never do this by IP when target is a CDN!!!

Guided walkthrough - Entry removed

Entry is removed. Next on the list is displayed.

Guided walkthrough - Manage safelists



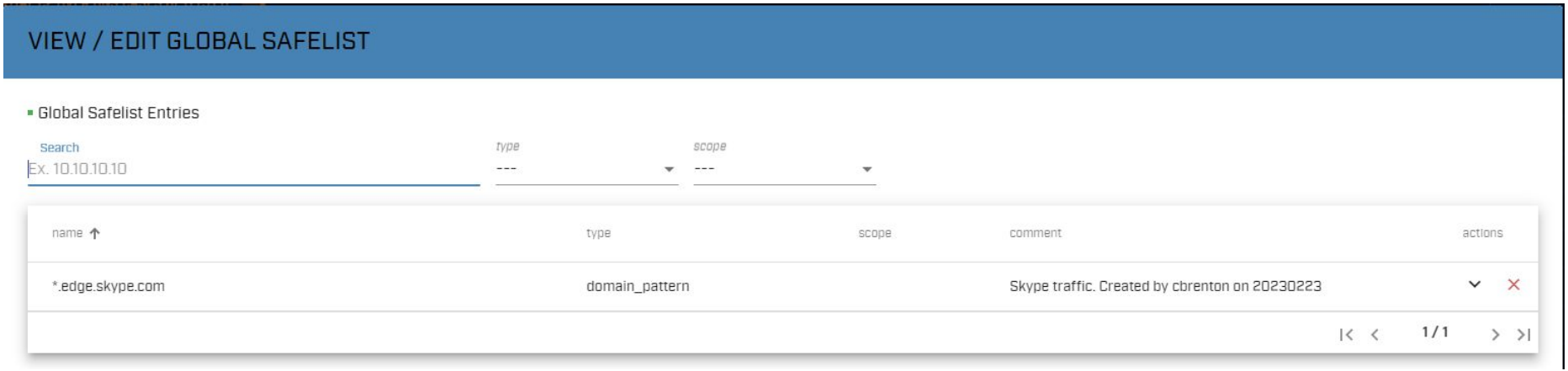
Return to the dashboard

Click the gear for Settings

Select "safelist"

Click "View/Edit" button

Guided walkthrough - View safelists



AC-Hunter CE supports 50 safelist entries

Guided walkthrough - Investigation

Highlight first entry

Click the first entry (Beacon score)

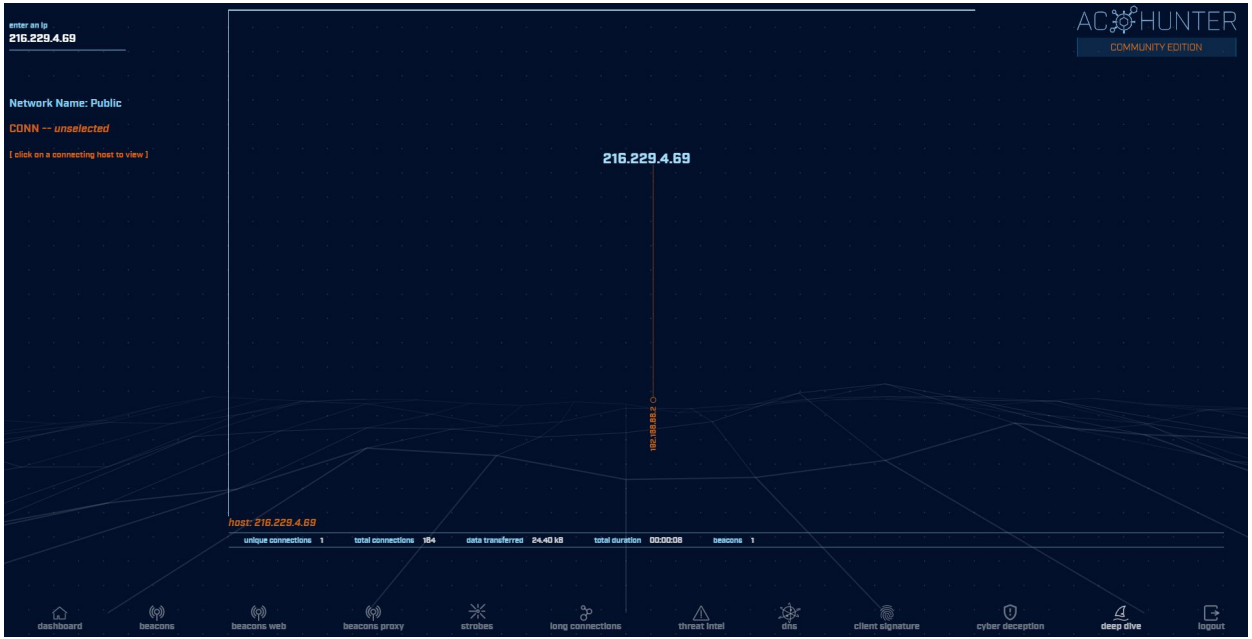
Guided walkthrough - Investigation

Clicking IP or FQDN opens investigation menu

Provide more data on subject

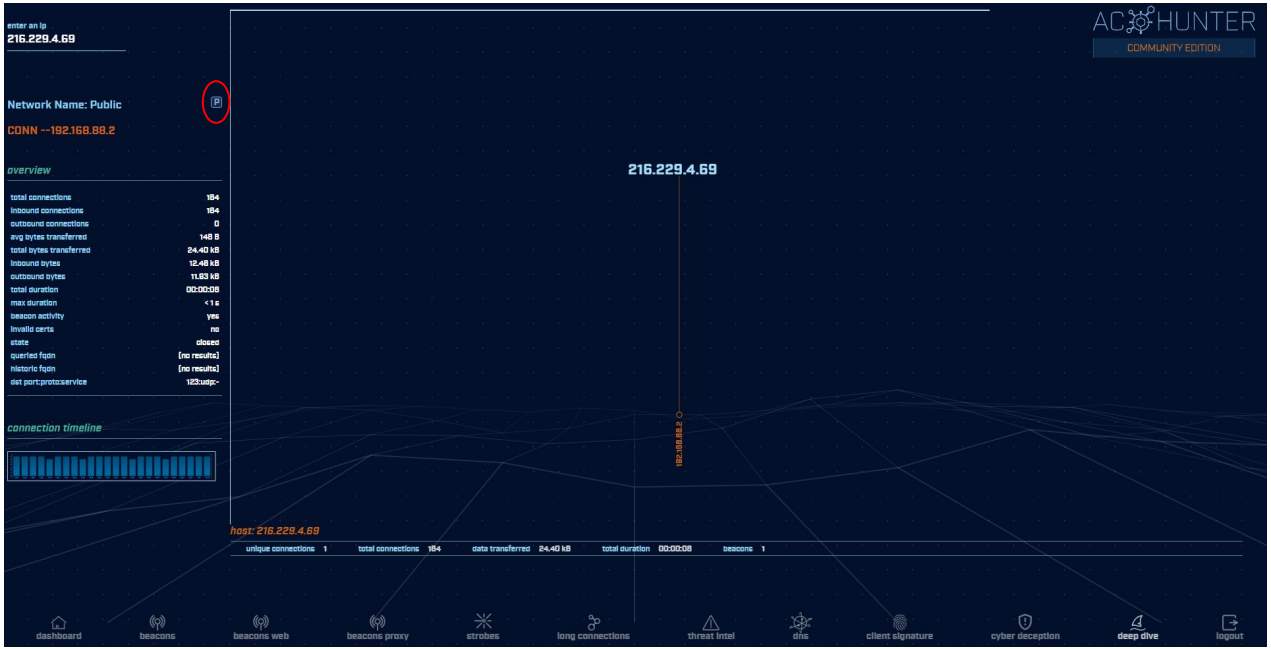
Start by clicking "deep dive"

Guided walkthrough - deep dive



Only internal host speaking to this IP

Guided walkthrough - more data

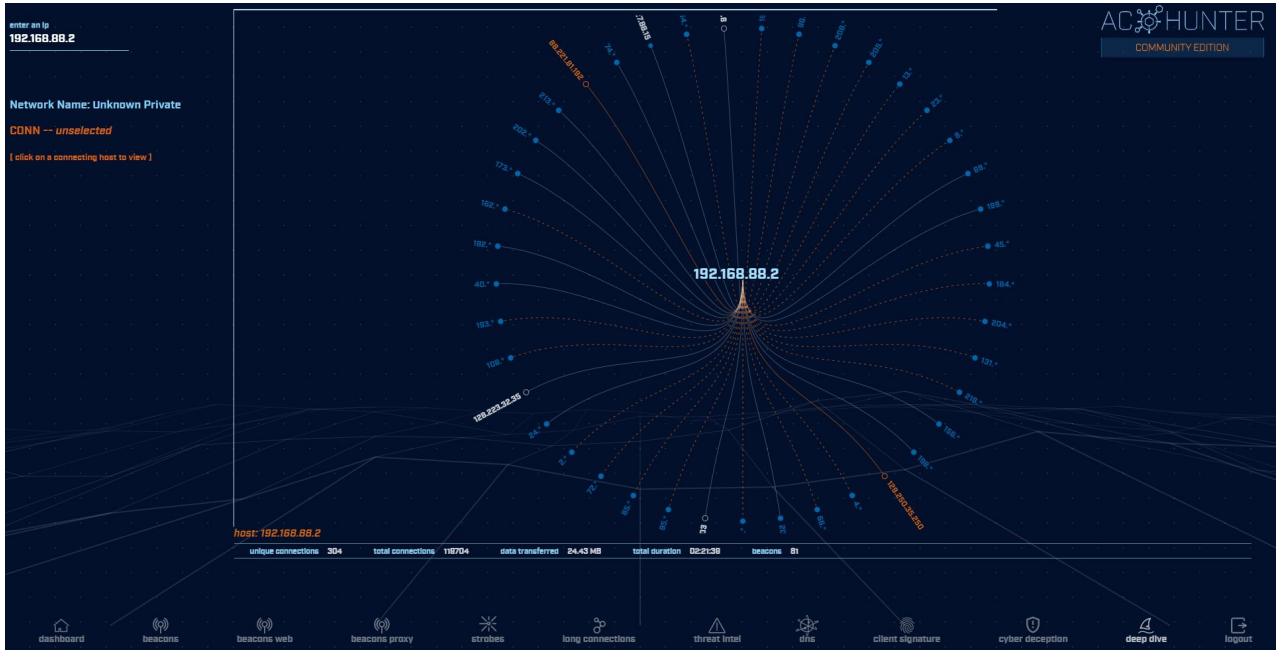


Click internal IP

Summary of comms shown

Click "P" to pivot

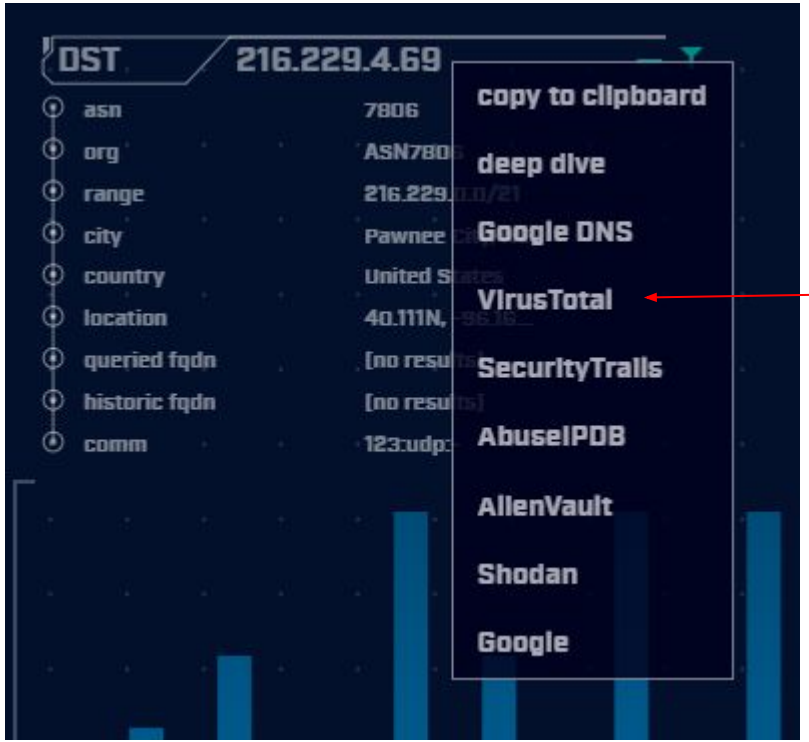
Guided walkthrough - pivot



Pivot changes view to other IP address

If you find a C2 server, use this to see if others are talking to it as well.

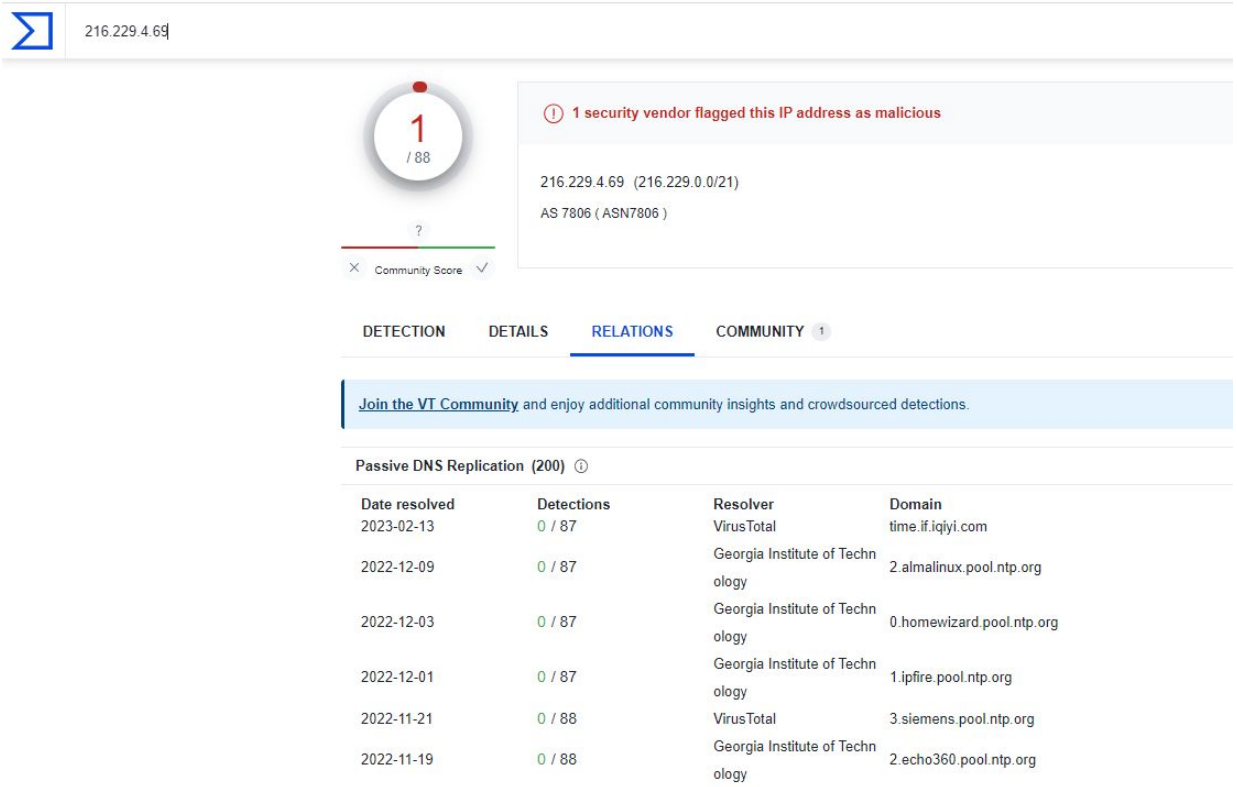
Guided walkthrough - Other options



Navigate back

Select VirusTotal

Guided walkthrough - Investigation



New tab opens

Passes IP/FQDN to external site for additional info

Guided walkthrough - Long conns

Return to dashboard

Open long connections module

Guided walkthrough - screen info

If you don't see data, check Search and Threshold. May need to clear values.

Note screen layout is similar.

Guided walkthrough - data import

- Follow along to import the data
- We have Zeek logs we want to analyze
- Let's get them imported in to ACH CE
- We'll use RITA to do the import
  - Yes, RITA is "under the hood"

Go to the lab1 directory

Navigate to the "lab1" directory

```
threat@ACH:~$ cd labs
threat@ACH:~/labs$ cd lab1
threat@ACH:~/labs/lab1$ pwd
/home/threat/labs/lab1
threat@ACH:~/labs/lab1$ ls
capture_loss.log  http.log            packet_filter.log
certs-remote.pem  known_hosts.log     software.log
conn.log          known_services.log  ssl.log
dhcp.log          loaded_scripts.log  stats.log
dns.log           notice.log          x509.log
files.log         ntp.log
threat@ACH:~/labs/lab1$ _
```

Importing Zeek logs into ACH

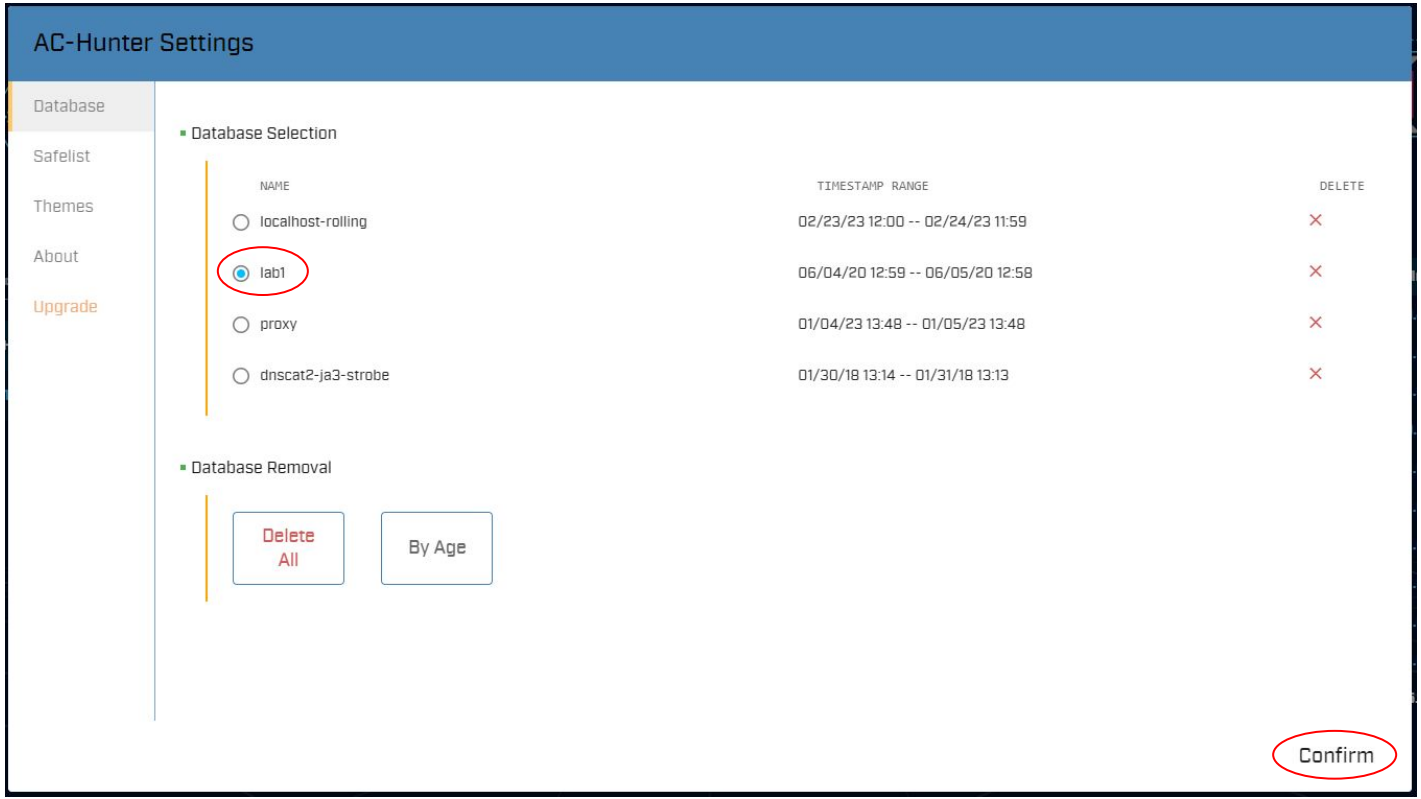
```
rita import <path to zeek logs> <database name>
```

```
threat@ACH:~/labs/lab1$ rita import *.log lab1
[sudo] password for threat:
Creating achunter_api_run ... done

        [+] Importing [/home/threat/labs/lab1/capture_loss.log
/home/threat/labs/lab1/conn.log /home/threat/labs/lab1/dhcp.log
```

…

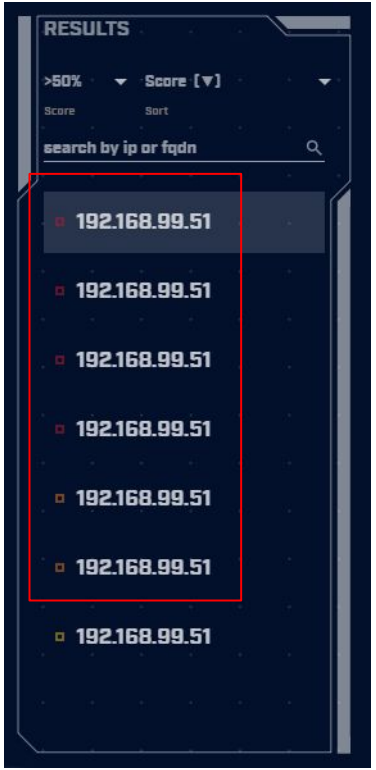
```
        [-] Indexing log entries ...
        [-] Updating metadatabase ...
        [-] Done!

threat@ACH:~/labs/lab1$
```

DB should now appear in ACH CE



Lab1

- Go to the beacon web module
- Six entries scored above 80
- Evaluate each of the 6
  - Spend about 60 sec max on each
  - Which entries look suspicious?
  - Which entries can be safelisted?
  - Make a list of each
- Stick with the UI
  - We'll dig into the logs in a later lab



Hints

- Go for the easiest ones first
- If you can decide in less than a minute, make a note and move to the next one
- Circle back to the hard ones after you've gone through everything

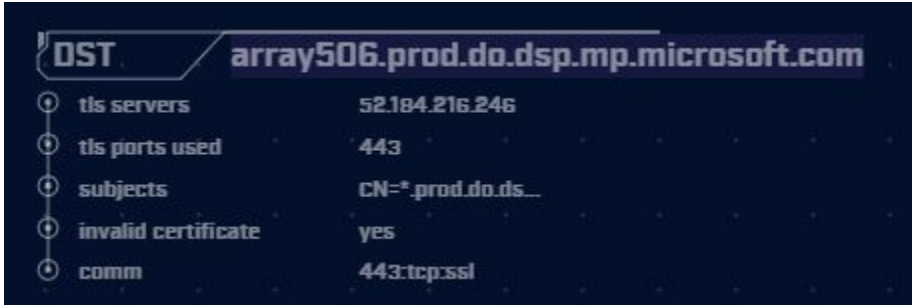
Lab1 - Answers

Lab1 answers - First entry

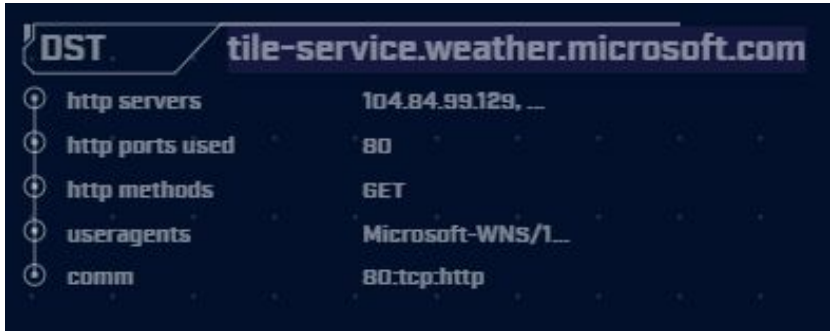
- Refer to previous slide
- Very high beacon score
- Lots of conns over 24 hours (3,011)
- Histogram is pretty flat
- User agent identifies as Windows 7
  - Could be legit but seems kind of old
- No host string
  - Should identify FQDN of Web server
- Well come back to this one

Lab1 answers - Second entry

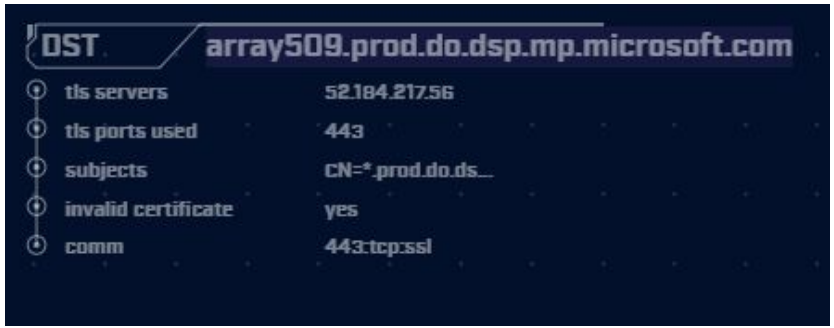
- MS delivery optimization host
- Used in Windows for patching
- Digital cert looks legit
- We could safelist this one



Lab1 answers - 3rd & 4th entry

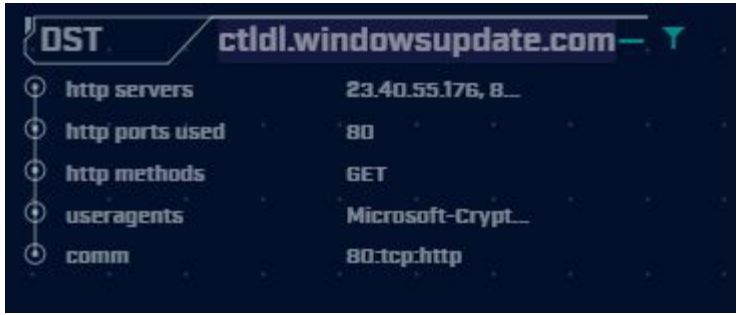


Windows tile services
This can be safelisted



Windows patching
Note this is similar to 2nd entry
"array509" versus "array506"
We can safelist both with a wildcard

Lab1 answers - 5th & 6th entry



Both are Windows patching
Note another "array"

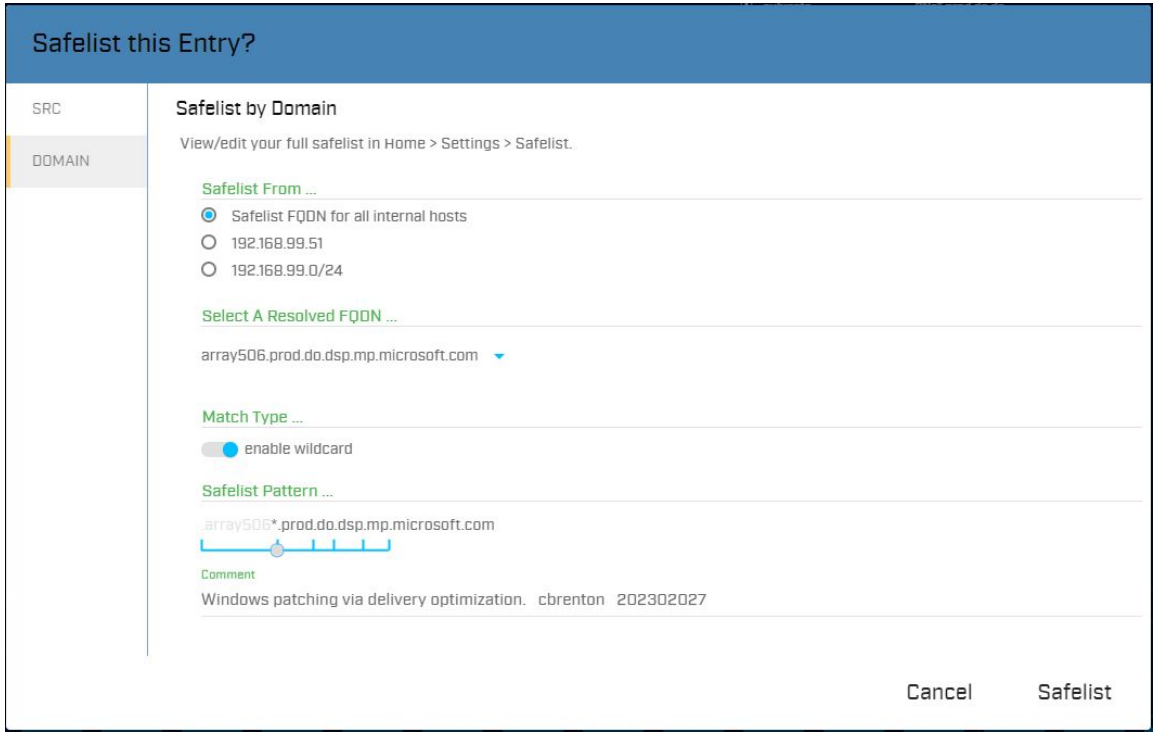
Next lab - Create safelist entries

- First entry looks suspicious
  - We will cycle back to it
- The rest look legit
  - Windows patching
  - Windows desktop tile services
- Let's safelist these last 5 entries
- Try this on your own

Lab hints

- Consolidate with wildcards
- You only need 3 safelist entries to cover all five targets
- Safelisting by FQDN is preferred
  - Updates when IP changes
  - Track through CDNs as required

Creating a safelist entry



Safelist settings

Any internal system

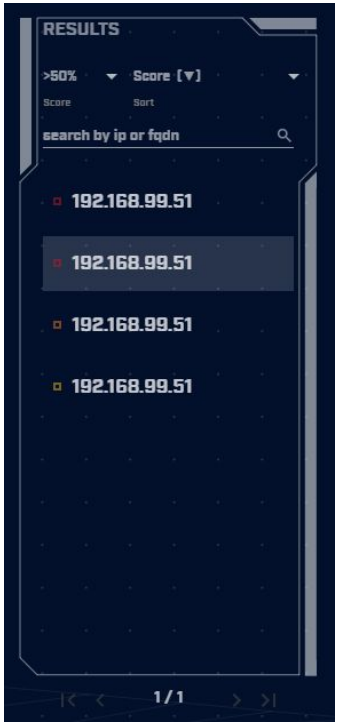
Wildcard match

Wildcard covers all "array" entries

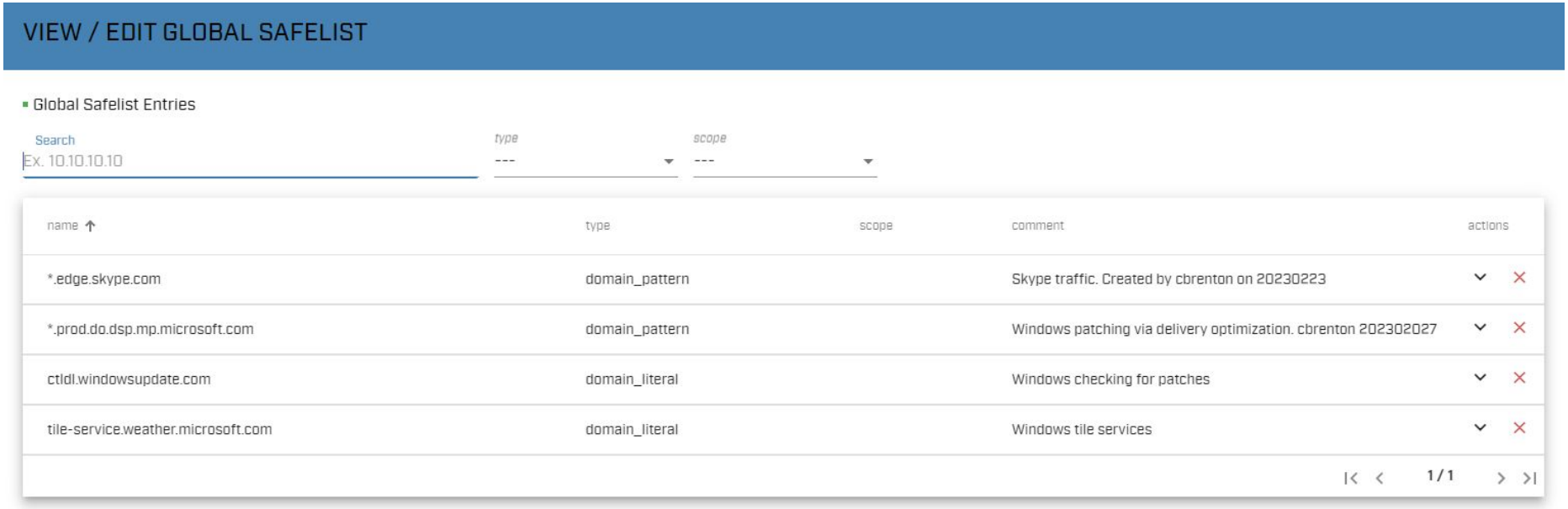
Don't forget Comment

Did you notice?

- The 1 safelist removed 3 entries
- All were "array" entries
- The wildcard covered all 3
- Create the last two needed



View safelists when complete



Completed safelist entries

Next lab!

- Still working with "lab1" dataset
- Go to "long connections module"
- Evaluate connections lasting > 5 hours
- Spend 60 seconds max on each
- Identify
  - Which look suspect and need further investigation?
  - Which can be safelisted?

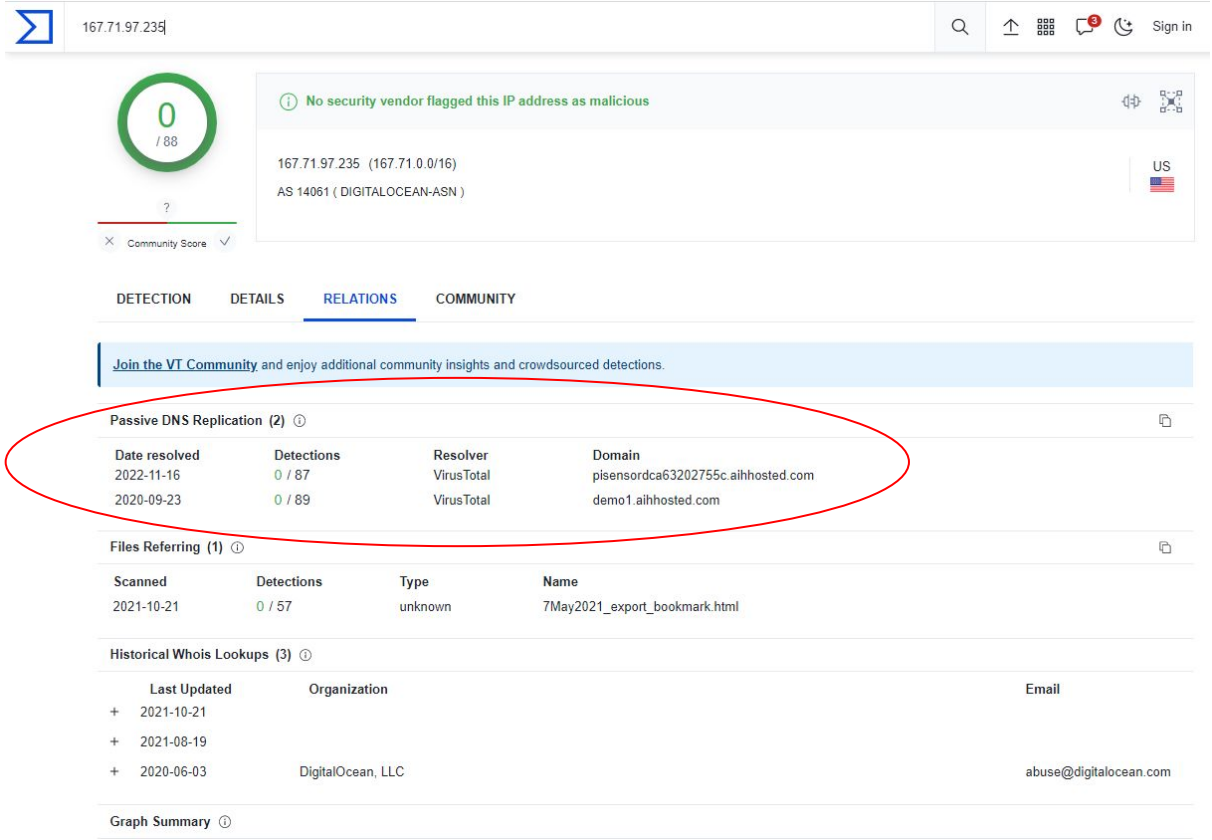
Hints

- Only two entries to work with
- Don't forget clicking an IP brings up the investigation menu
- What is known about the external IP?
- Could this host serve a legitimate business purpose?

Answers - Some basic info

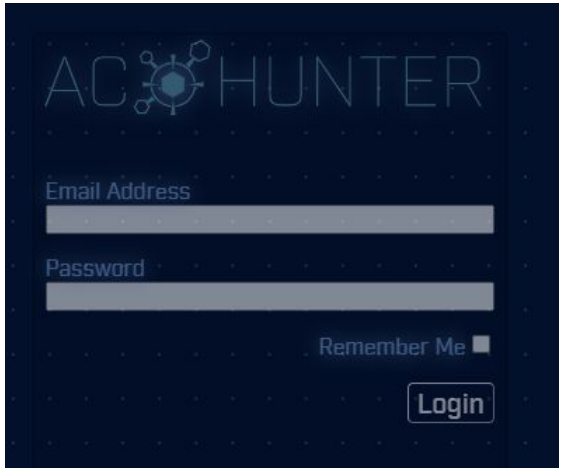
- NO FQDN entry identified for either IP
- "comm" does not identify protocol
- ACH stores this data for 24 hours
  - FQDN queried via DNS
  - App protocol during initial negotiation
- After 24 hours, both labeled as unknown
- We would need to go back through the Zeek data to when the conn started

Lab answers - 1st IP



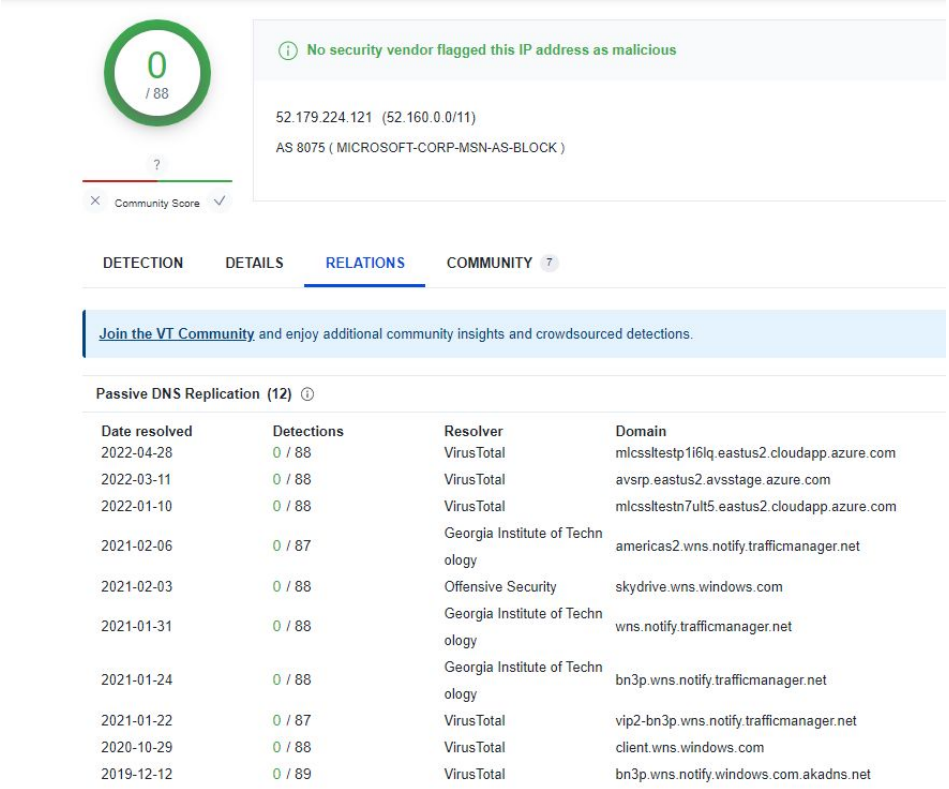
What if I visit this IP or domain?

Connect from a non-work related IP



Target produces an "AC-Hunter" login
www.aihhosted.com redirects to Active Countermeasures
Can we identify a business need with this tool or domain?

Answers - 2nd IP



Looks like Windows notification services

Standard Windows Service

Answers - Sanity check

- 1 suspect beacon
- 5 beacons with a business need
- 1 long conn that's probably OK
  - demo1.aihhosted.com
- 1 long conn that can be safelisted
  - Windows Notification Service
  - Safelist the destination IP address
- That just leaves the first beacon

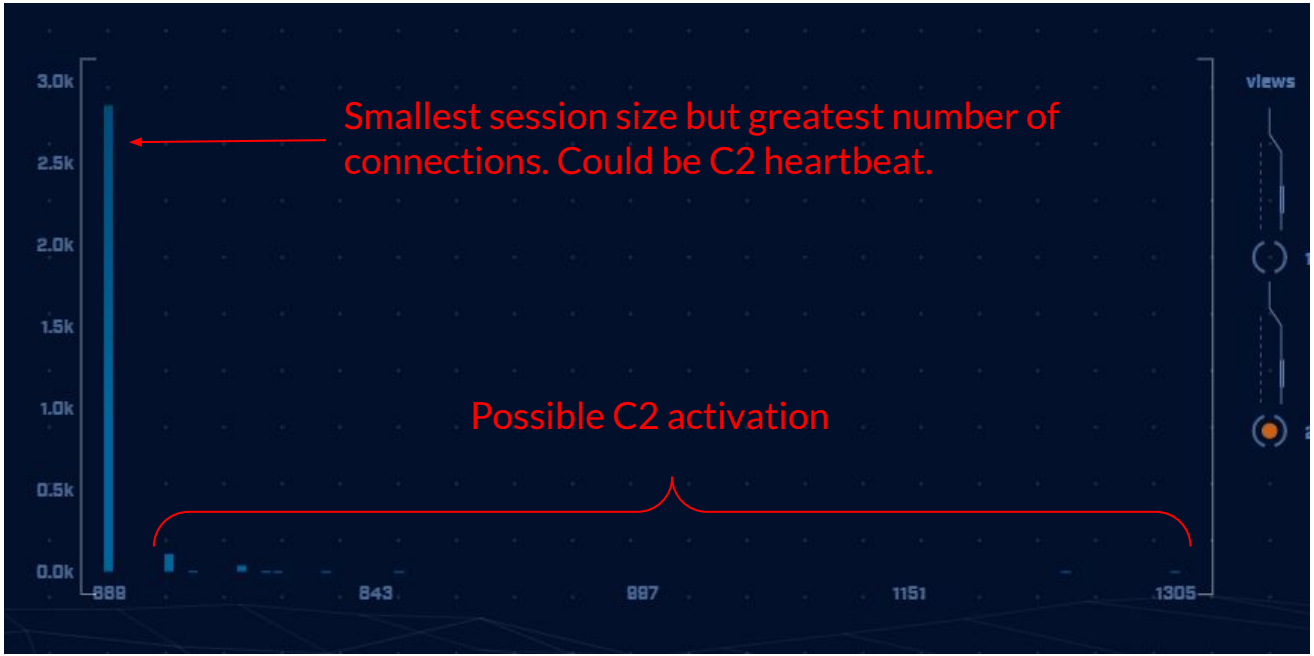
Another lab - Deep dive on beacon

- The IP 104.248.234.238 is suspect
- Let's deep dive on this connection
- What can we learn about this IP?
- Anything odd about the session?
- If you are running the VM:
  - Additional data in Zeek logs
  - Anything useful?
- Determine if comms are suspect or not

Hints

- User agent says Windows 7
- Is this consistent will all other conns?
- Perform a session size analysis
  - View 2 on beacon screen
  - Does this look like C2?
- What does Zeek show for a payload?
- Any other useful info?

Answers - session size analysis



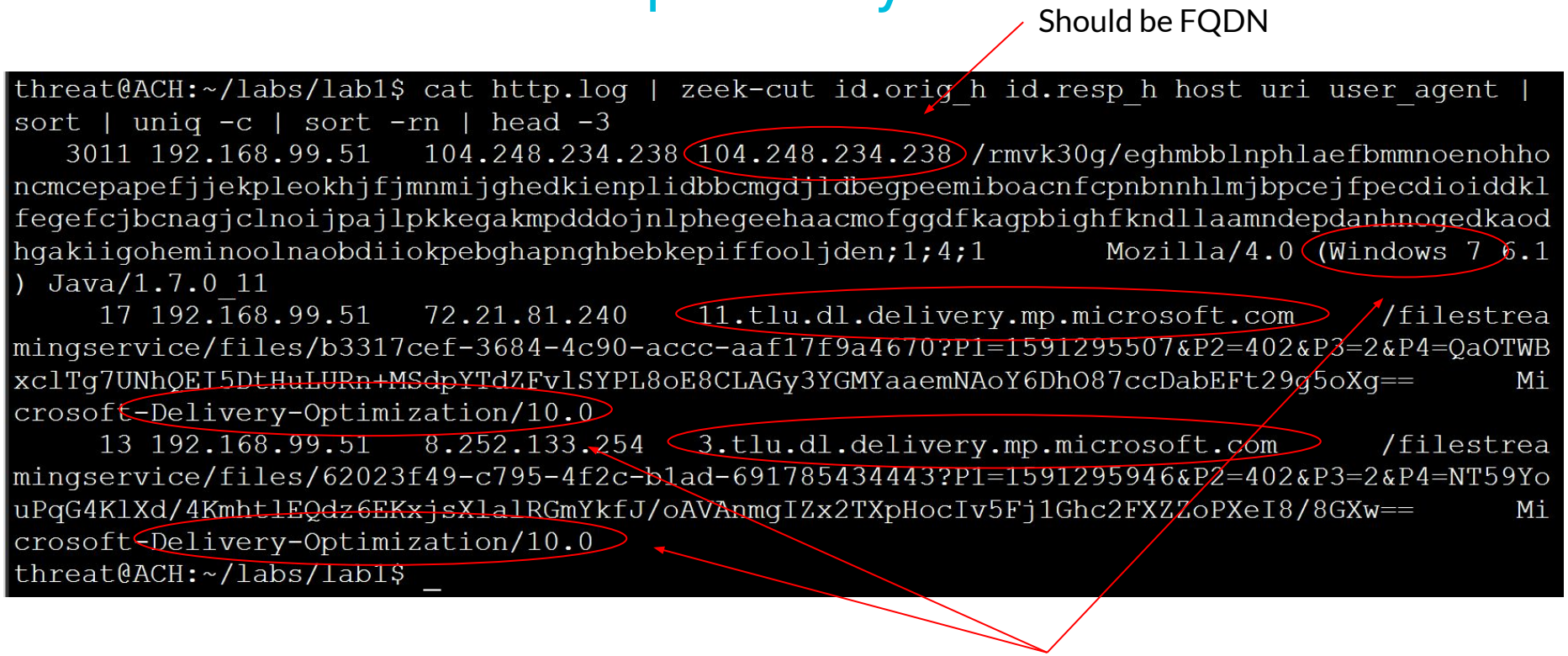
Sessions do have potential C2 attributes

Lab answers - suspect sessions

- Confirmed no FQDN query prior to connection
- This is highly suspect

```
threat@ACH:~/labs/lab1$ cat dns.log | zeek-cut query answers | grep 104.248.234.238
threat@ACH:~/labs/lab1$
```

Answers - http analysis



Answers - User agent analysis

```
threat@ACH:~/labs/lab1$ cat http.log | zeek-cut id.orig_h id.resp_h user_agent | sort | un
iq | cut -f 3 | sort | uniq -c | sort -rn
     29 Microsoft-WNS/10.0
     16 Microsoft-Delivery-Optimization/10.0
      8 Microsoft-CryptoAPI/10.0
      1 WicaAgent
      1 Mozilla/4.0 (Windows 7 6.1) Java/1.7.0_11
threat@ACH:~/labs/lab1$ _
```

Claims to be Windows 7 when speaking to this one IP
Claims to be Windows 10 for all other destination IP addresses

Answers - uri analysis

```
threat@ACH:~/labs/lab1$ cat http.log | zeek-cut id.orig_h id.resp_h uri | grep 104.248.234
.238 | sort | uniq -c | sort -rn
   3011 192.168.99.51   104.248.234.238 /rmvk30g/eghmbblnphlaefbmmnoenohhoncmcepapefjjekpl
eokhjfjmnmijghedkienplidbbcmgdjldbegpeemiboacnfcpnbnnhlmjbpcejfpecdioiddklfegefcjbcnagjcln
oijpajlpkkegakmpdddojnlphegeehaacmofggdfkagpbighfkndllaamndepdanhnogedkaodhgakiigoheminool
naobdiiokpebghapnghbebkepiffooljden;1;4;1
threat@ACH:~/labs/lab1$ _
```

All 3,011 connection are this same really long string

Final answer

- Connections with 104.248.234.238 are highly suspect
  - No FQDN queries
  - 3,011 connections with strong beacon attributes
  - Shifting user agent string
  - No "host" field in HTTP header
  - Long convoluted URI string
  - Googling "rmvk30g" returns "Fiesta EK"
- All other entries can be safelisted

It's worth noting

- Capture contained 14,000+ connections
- Only one was "evil"
- We found it pretty quickly with ACH CE

Next lab!

- Let's move to the lab2 directory
- VM users will need to import the data
- After data import, select "lab2" database and hunt the data
- Use the last set of labs as a guide

```
threat@ACH:~/labs/lab1$ cd ../lab2
threat@ACH:~/labs/lab2$ rita import *.log lab2_
```

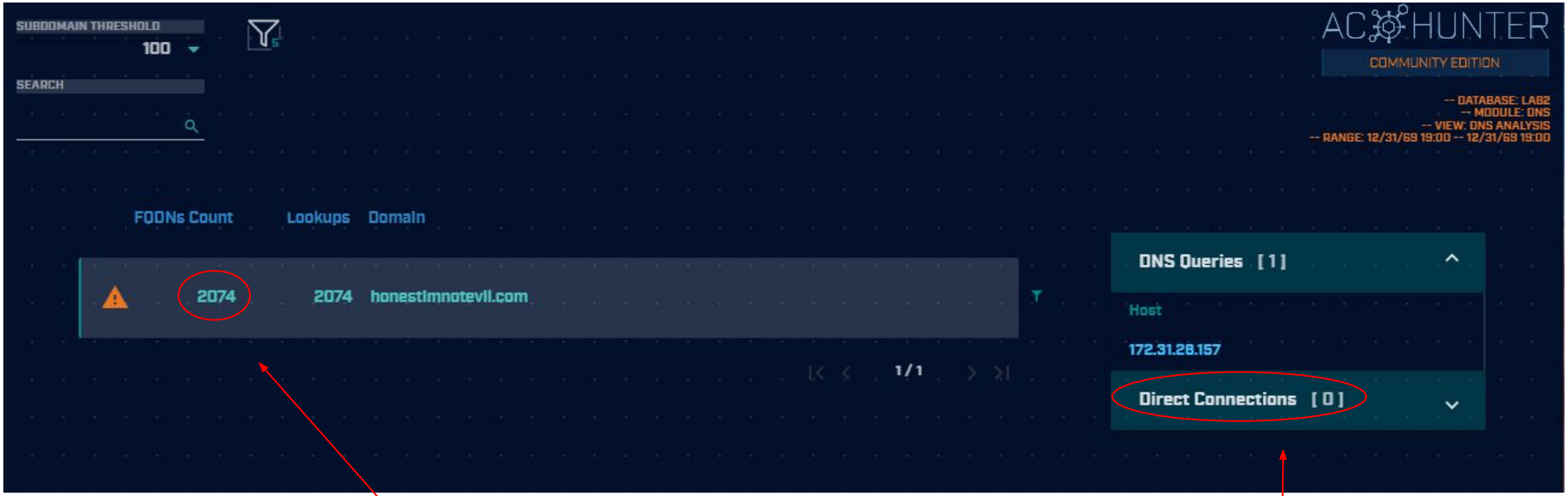
Hints

- May appear there is no results
- Check the top left of screen
- Pointing you to DNS module

Lab answers - C2 over DNS

- It looks like there is no data
- No individual IPs are listed
- Check top left of screen
- Indicates to check the DNS module
- C2 over DNS is presented differently
  - Source may be resolver, not infected client
  - Multiple src IPs if multiple resolvers are used
  - Results are consolidated for accuracy

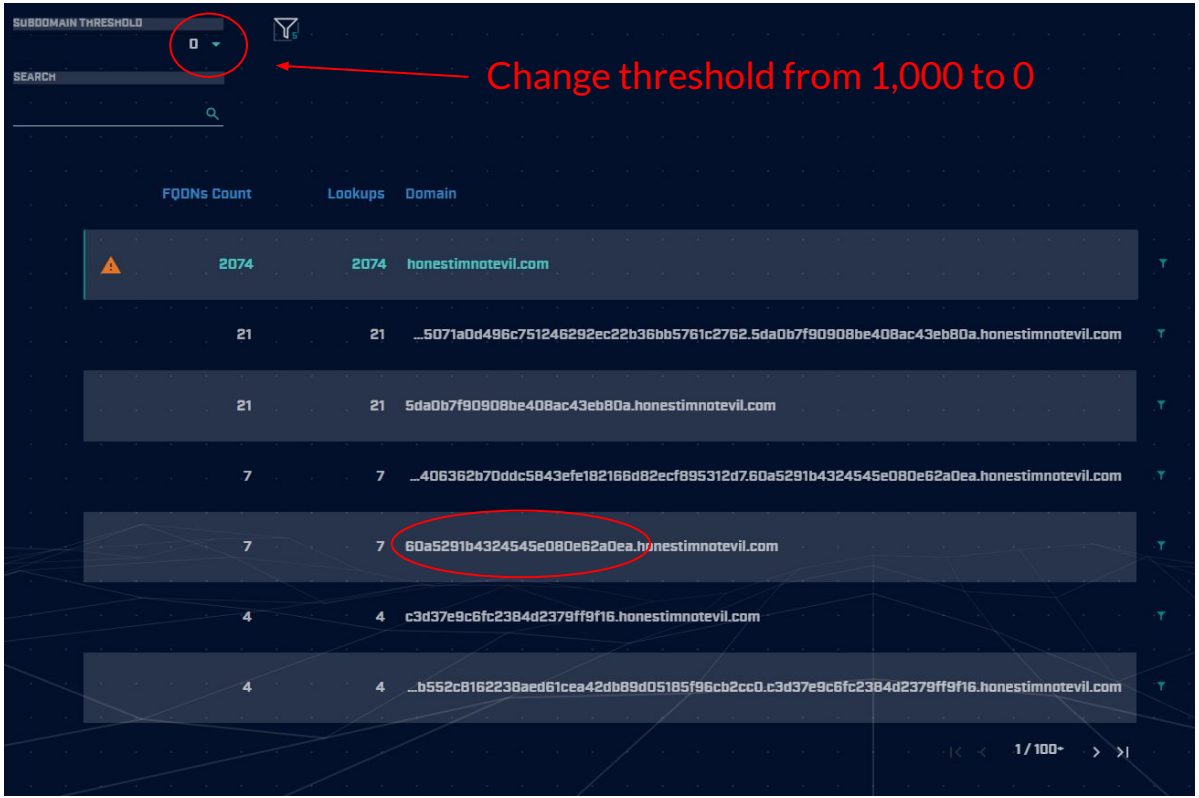
Answers - C2 over DNS results



More unique resource records than reasonable

No users accessing resources

Answers - drill down on DNS



Host name is Hex characters

Not usually a naming convention people use

Answers - Final

- Potential C2 over DNS
- Need to check source IP
  - Is it a client system?
  - Is it a DNS resolver?
  - True source must be identified
- Looks like dnscat2

Next set of labs!

- Let's move to the lab3 directory
- VM users will need to import the data
- After data import, select the "lab3" database and hunt the data
- Use the last set of labs as a guide

```
threat@ACH:~/labs/lab3$ cd ../lab2
threat@ACH:~/labs/lab2$ cd ../lab3
threat@ACH:~/labs/lab3$ rita import *.log lab3
```

Hints

- Repeat the process we've been using
- Where do you see high scores on the dashboard?
  - Investigate highest scores first
- Remember how we identified C2 beacons

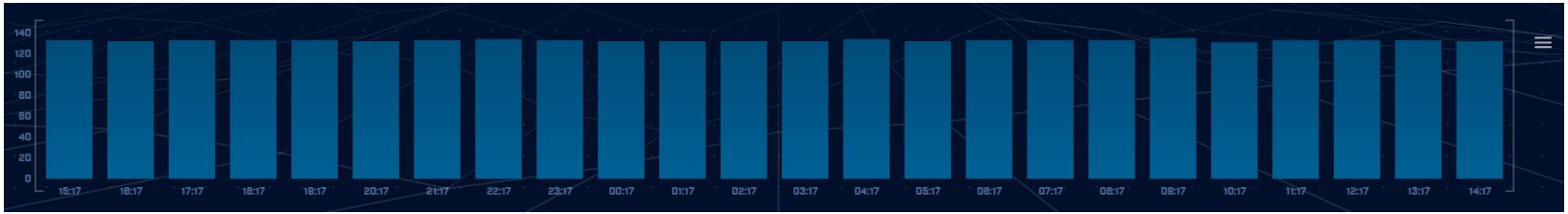
Answers - Start with beacon web

That's not quite a Skype domain
Feel a bit scammy.

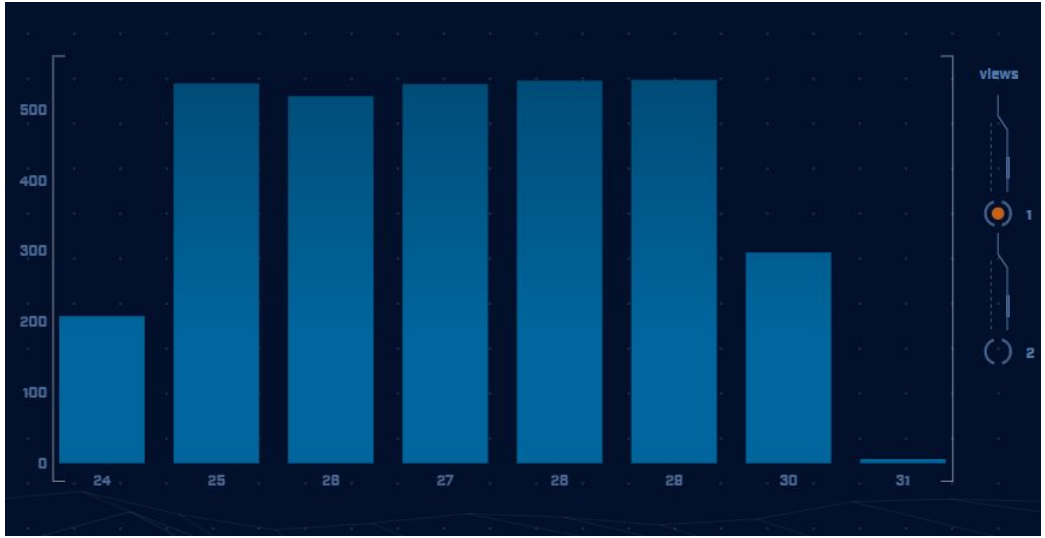
User agent is "Internet Explorer".
Not a valid user agent.

Answers - Skype like FQDN

Time histogram clearly shows a beacon



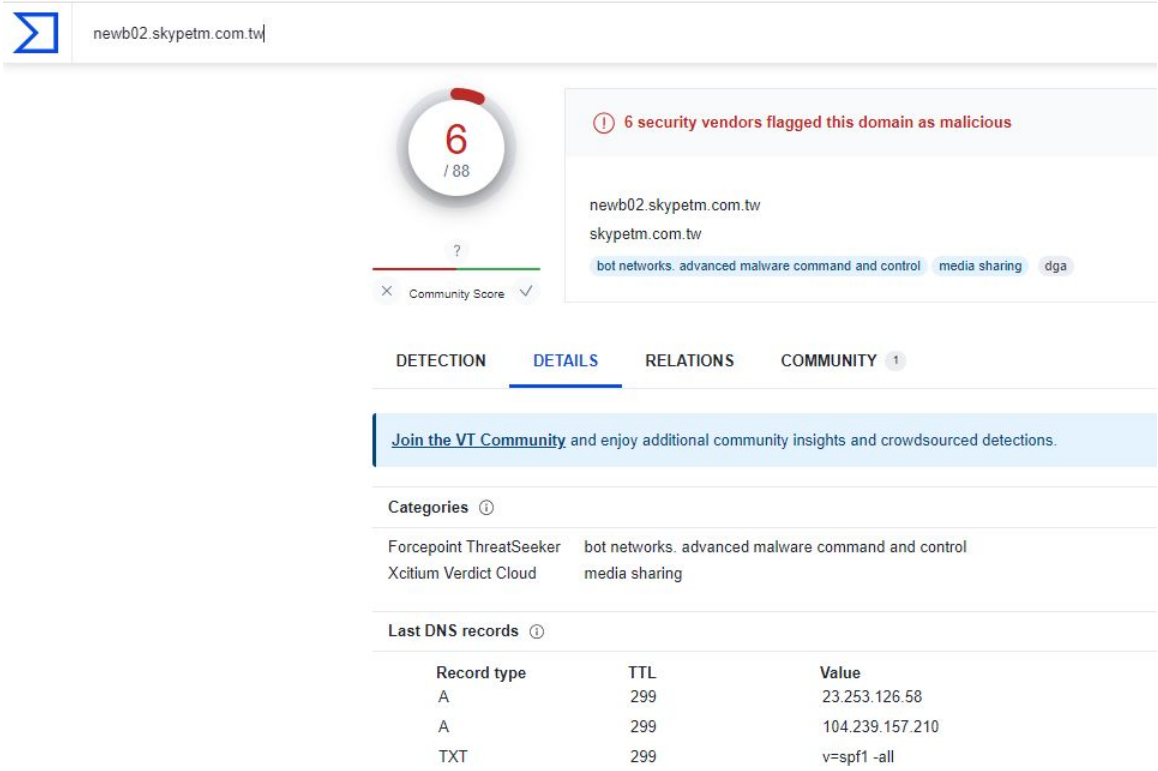
Answers - jitter



Connection dwell time is being jittered

The curve indicates Cobalt Strike

Answers - This is not good



Answers - Let's move on

- We clearly have an HTTP beacon
  - Histogram is flat
  - User agent looks bogus
  - FQDN looks bogus
- We have enough data to trigger an incident response on our system
- Let's check for anything else

Answers - MS Office traffic

Can be safelisted if we use MS Office

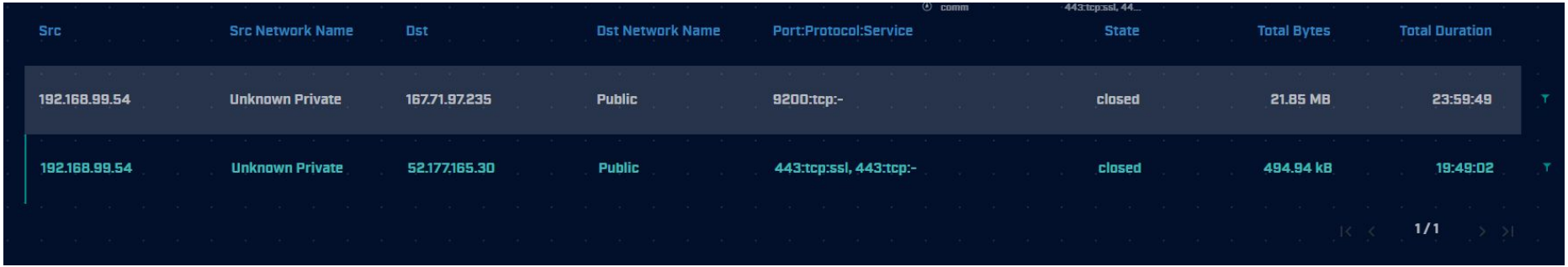
Answers - OpenDNS

Two similar entries
DNS queries to OpenDNS

Do we use OpenDNS for DNS?
Have we purchased their security service?

If yes to the above, safelist.
If no to the above, investigate internal endpoint.

Answers - Long connections



Src	Src Network Name	Dst	Dst Network Name	Port:Protocol:Service	State	Total Bytes	Total Duration
192.168.99.54	Unknown Private	167.71.97.235	Public	9200:tcp:-	closed	21.85 MB	23:59:49
192.168.99.54	Unknown Private	52.177.165.30	Public	443:tcp:ssl, 443:tcp:-	closed	494.94 kB	19:49:02

1 / 1

These are the same entries we had in the first lab.

May not appear if you safelisted them.

If you want to keep practicing

- Check our malware of the day blog
- Skip to the bottom, download the 24 hour long pcap file
- Process the pcap with Zeek
  - zeek -C -r <name of pcap> local
- Import into AC-Hunter
- When done, check the blog for answers
  - Did you miss anything?

https://www.activecountermeasures.com/?s=malware+of+the+day

Interested in a demo?

- Enterprise version has a lot more features
- Type "demo" in Zoom chat (not Discord) to learn more
  - Or email questions@activecountermeasures.com
- Huge refresh coming out over the next few months!
  - Were you here for the sneak peek?

Closing thoughts

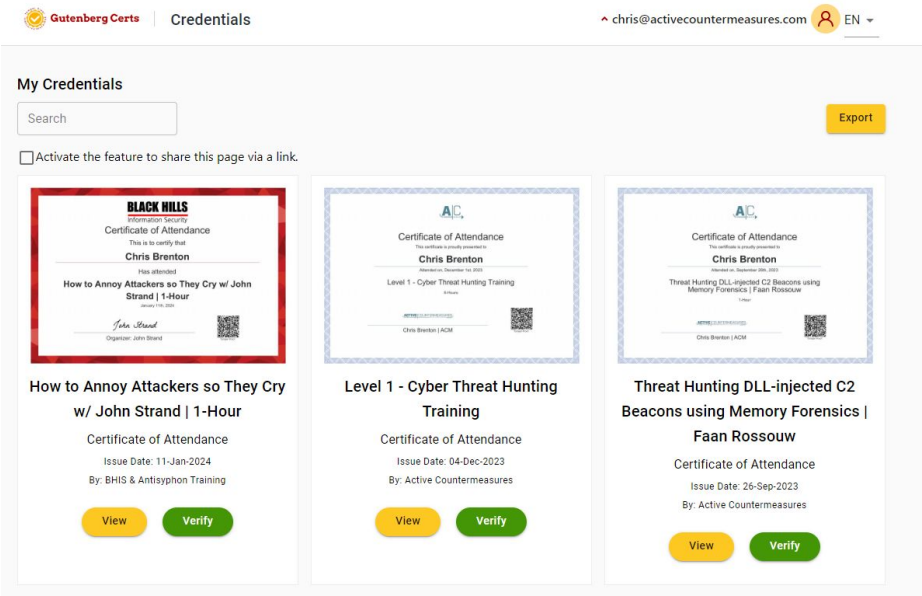
- Remember the process
  - Identify connection persistency
  - Identify business need if present
  - Investigate external IP
  - Investigate internal IP
- Disposition each IP
  - Pretty certain it's still pristine
  - Pretty certain it's compromised
- Don't cross the passive/active line

Classes I'm teaching

- Intro to Packet Decoding
  - IP headers from a security perspective
  - April 23rd - 26th
  - https://www.antisyphontraining.com/live-courses-catalog/getting-started-in-packet-decoding-chris-brenton/
- Advanced Threat Hunting
  - Next step up from this course, mostly C2 labs
  - May 21st - 24th, then Aug 13th - 16th
  - https://www.antisyphontraining.com/advanced-network-threat-hunting-w-chris-brenton/
- Security Compliance and Leadership
  - Getting funded, C level communications, team management
  - Aug 22nd & 23rd, to be announced on Antisyphon site
  - https://www.antisyphontraining.com/live-courses-catalog/security-leadership-and-management-w-chris-brenton/
- Next run of this class is…TBD

When will I get my cert?

Certs go out within 24 hours or retrieve on Gutenberg Certs
https://myaccount.gutenbergcerts.com/dashboard



Thank you for attending!

- Thank you for sharing your valuable time with us today
- We hope the class has been helpful
- The team will monitor Discord for any last minute question