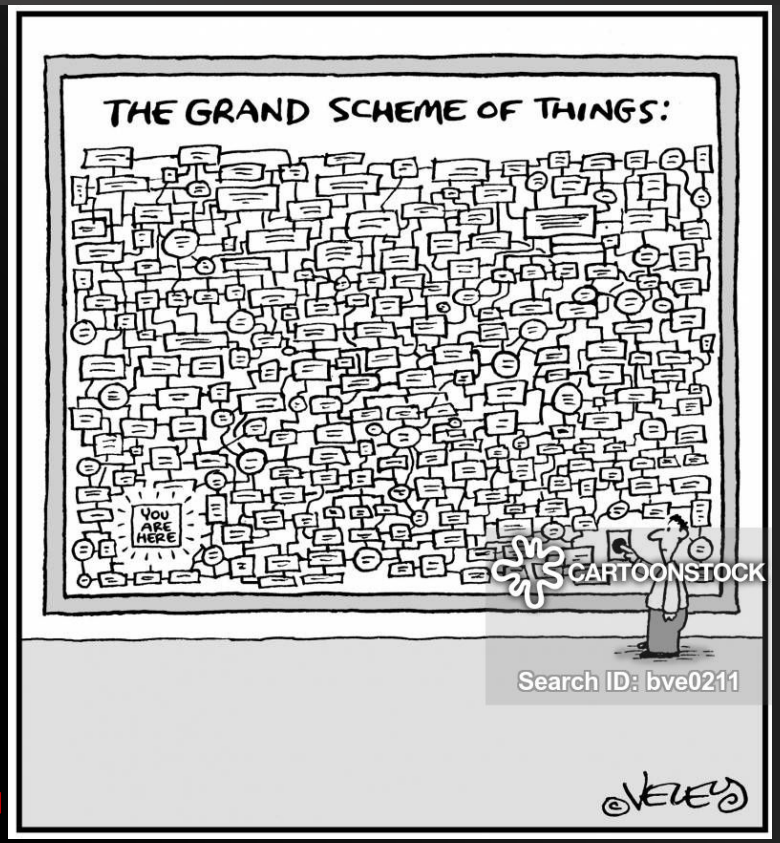
You Are Compromised? What Now?

John Strand

Why?

- First steps are tough..
- Mistakes and paralysis
- Need to keep moving
- Need to have a plan
- I want to cover some basic first steps

The Wrong Way...

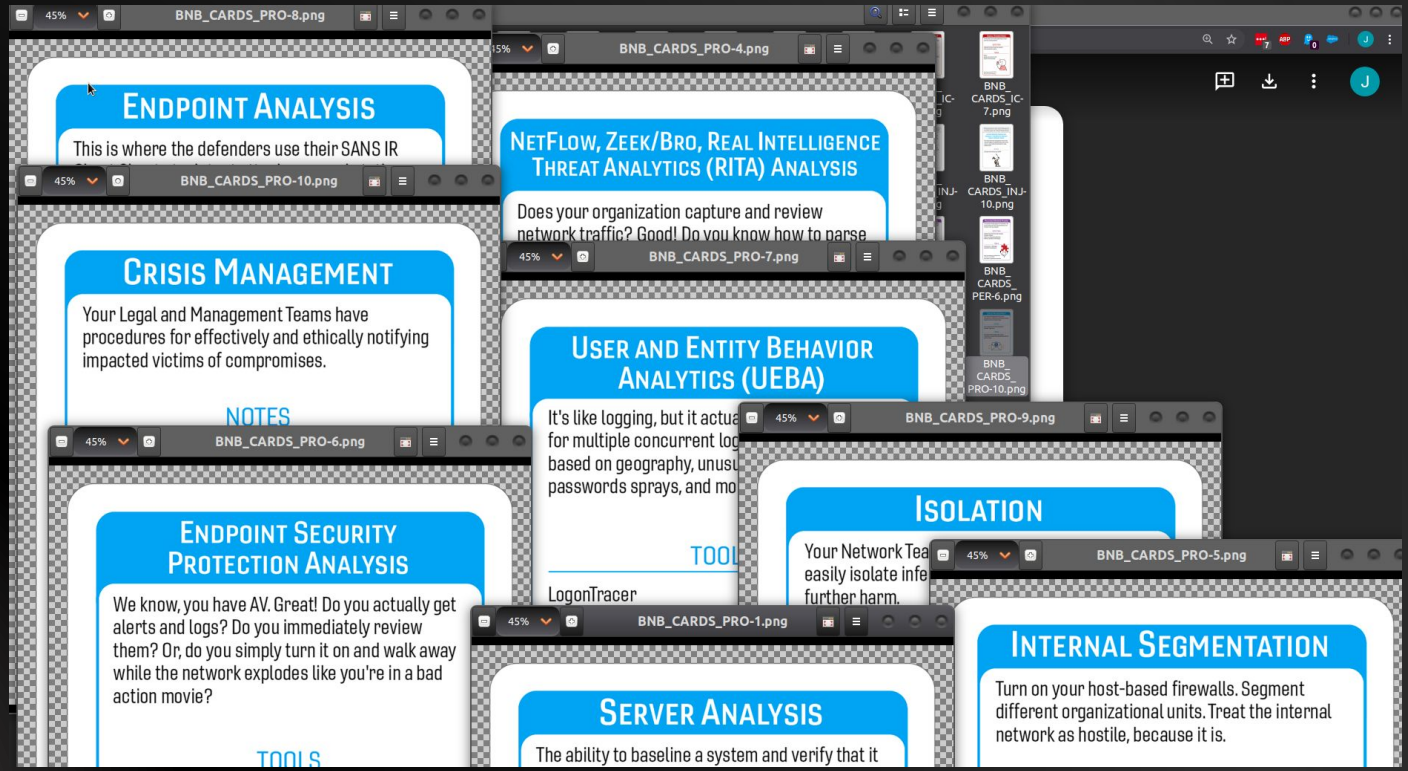


The Right Way

BLACK HILLS Information Security
CELEBRATING 10 YEARS
•2008-2018•

Backdoors & Breaches

IR “Legos”



Don't Panic

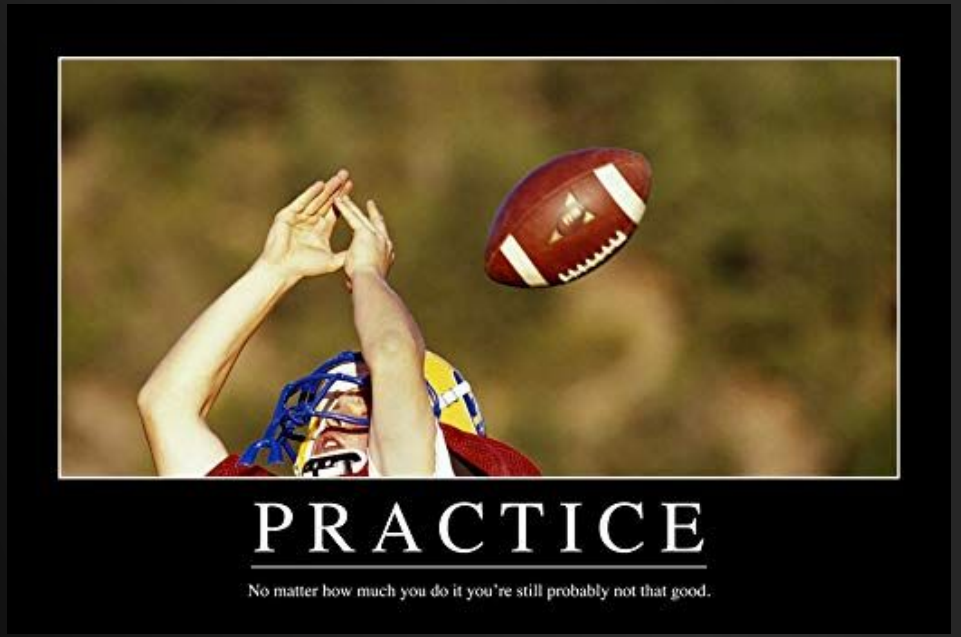
- First step… Don’t freak out
- I said DON’T FREAK OUT
- DON’T FREAK OUT!!!!!!!
- This only comes with practice
- Think weapons training
- Don't wait for an incident to try tools you have read about
- Memory forensics, Deep Blue CLI, IR Scripts, Logontracer, etc.

Let's Get Some Things Out Of The Way

- Secure the area
- Notify appropriate officials
  - We are not covering IR comms
  - Check out CyberCPR
- Start recording everything in a log book
- Pull together the right team
- There is a lot of structural stuff
- All for another webcast

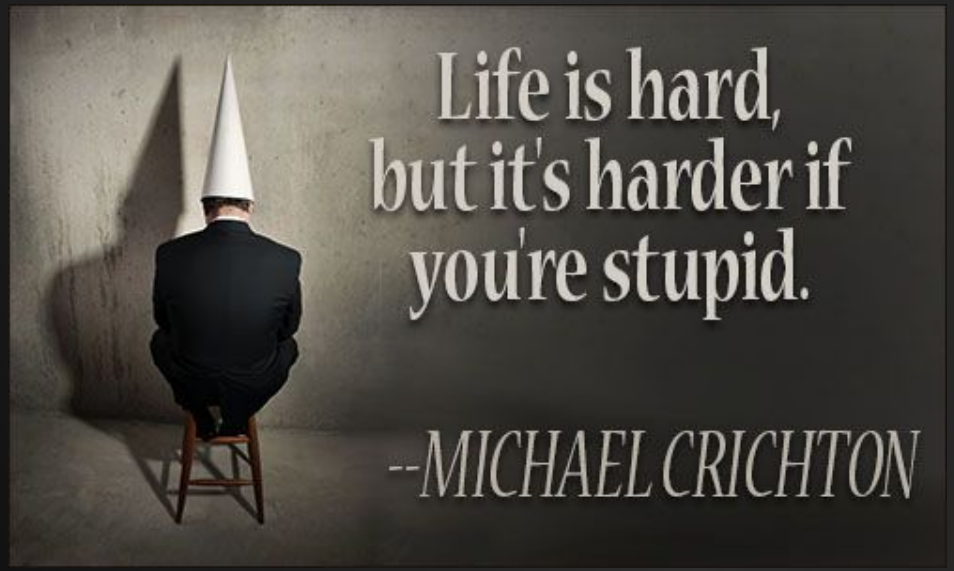
Where Are Your Logs?

- Time to pull your logs
- I mean all of them
- Systems, Servers, Services
- Network logs
- Log, Log, Log
  - But…
- Getting the right log is a pain
- Drill baby, drill….

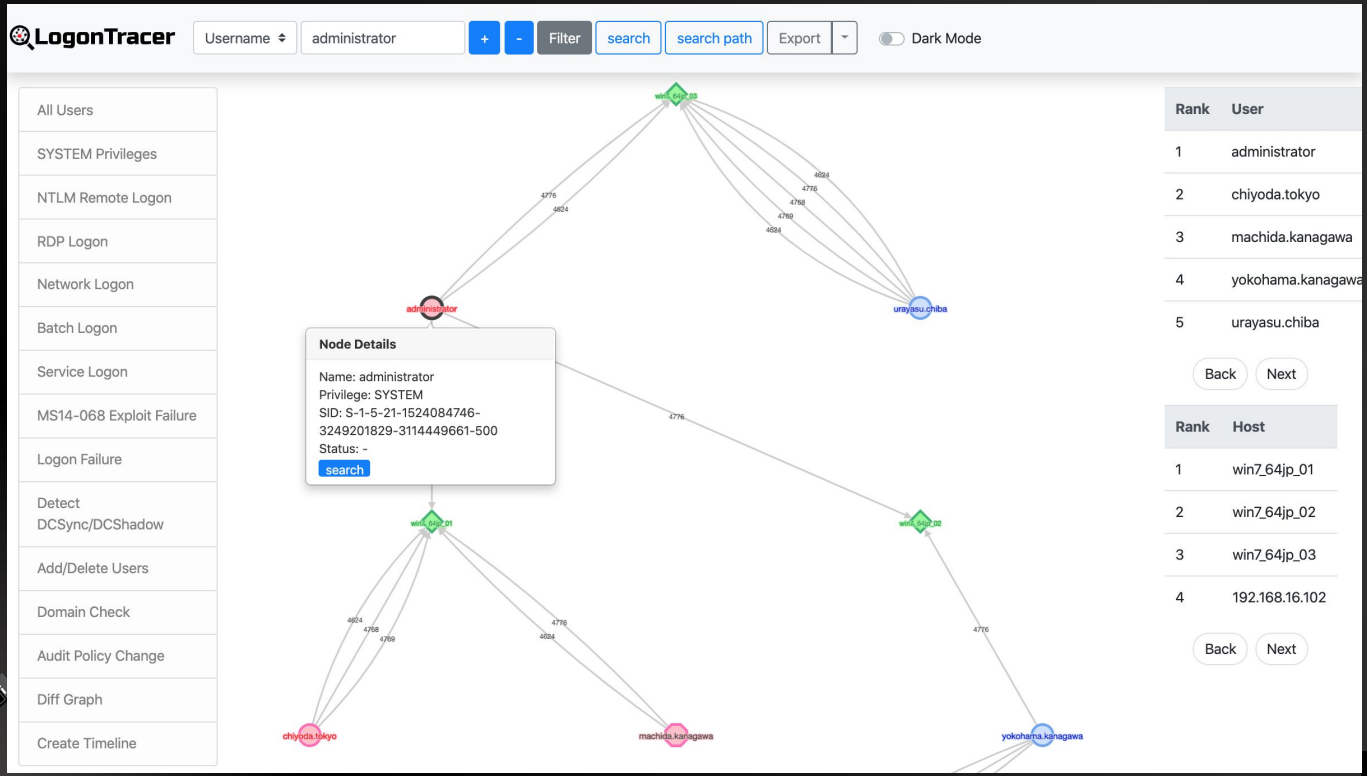


AD Logs

- Time to tie an account (or accounts) to activity
- UEBA is your friend
- “But it’s noisy..” Yes, security is hard
- You know what is harder? Doing this without UEBA
- Activity path



LogonTracer



LogonTracer

Rank	User
1	administrator
2	machida.kanagawa
3	yokohama.kanagawa
4	urayasu.chiba
5	chiyoda.tokyo

Rank	Host
1	win7_64jp_01
2	win7_64jp_02
3	192.168.16.101
4	192.168.16.103
5	win7_64jp_03
6	192.168.16.102

LogonTracer

Timeline | Username | administrator | + | - | Table | search | all | Download ▾

	2017																			
	9																			
	29(Fri)									30(Sat)										
Username	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10
yokohama.kanagawa	0	4	0	4	4	0	4	0	4	0	8	4	0	4	0	4	0	4	8	0
sysg.admin	2	0	2	3	0	2	0	3	0	2	0	4	2	0	2	1	2	0	3	1
utsunomiya.tochigi	1	2	2	0	3	0	2	0	4	0	2	2	1	2	0	2	2	2	0	2
urayasu.chiba	8	0	4	0	8	0	4	0	4	4	0	4	5	0	7	0	4	0	4	4
nagoya.aichi	0	1	0	7	4	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0
chiyoda.tokyo	0	0	4	0	4	0	4	4	0	4	0	8	4	0	4	0	4	0	4	5
urawa.saitama	4	0	8	0	4	0	4	3	0	4	0	4	8	0	4	0	4	0	4	4
sapporo.hokkaido	4	0	4	0	4	0	4	0	4	4	0	8	0	4	0	4	0	4	4	0
naha.okinawa	0	2	3	0	2	2	1	2	0	2	4	0	2	2	1	2	2	0	3	2
sakai.osaka	0	4	0	4	4	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0
hakata.fukuoka	0	4	0	8	0	4	0	4	0	4	4	0	8	0	4	4	0	4	4	0
maebashi.gunma	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
machida.kanagawa	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
mito.ibaraki	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

	2017																							
	9													10										
	30(Sat)													1(Sun)										
Username	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10
yokohama.kanagawa	4	0	4	15	0	5	0	4	8	0	4	0	4	4	0	4	0	4	0	8	0	4	4	0
sysg.admin	2	3	0	0	6	36	0	3	0	2	2	1	3	0	2	1	2	0	2	3	0	2	0	4
utsunomiya.tochigi	3	0	2	9	1	2	0	0	3	2	0	2	1	2	0	2	2	2	2	0	3	0	2	0
urayasu.chiba	0	4	0	4	0	9	0	0	4	0	4	4	0	8	0	4	0	4	4	0	4	0	8	4
nagoya.aichi	5	0	7	8	4	0	0	4	0	4	0	8	0	4	0	0	0	0	0	0	6	0	3	0
chiyoda.tokyo	0	7	0	11	5	0	0	0	4	0	5	0	3	1	0	1	0	0	0	0	0	0	0	0
urawa.saitama	0	5	0	10	0	5	0	0	4	0	4	8	0	4	0	4	0	4	4	0	4	0	8	4
sapporo.hokkaido	8	0	4	22	0	4	0	4	4	0	5	0	6	0	4	0	3	4	0	4	0	8	4	0
naha.okinawa	0	3	3	20	0	2	0	2	2	0	4	0	2	2	1	2	2	0	3	2	0	3	3	0
sakai.osaka	4	0	8	11	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0	4	8	0	4	0
hakata.fukuoka	4	0	8	11	0	5	0	4	0	4	5	0	7	0	4	0	4	4	0	4	0	8	0	4
maebashi.gunma	0	0	0	3	20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
machida.kanagawa	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
mito.ibaraki	0	0	0	6	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

BLACK HILLS Information Security CELEBRATING 10 YEARS • 2008-2018 •

Backdoors & Breaches

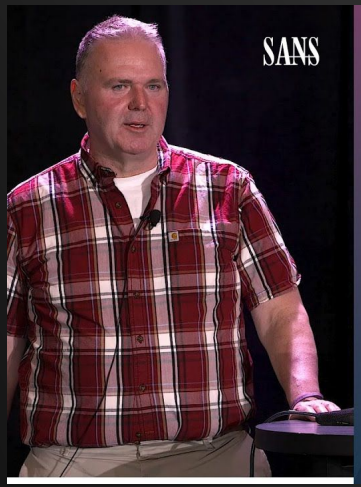
DeepBlueCLI

- https://github.com/sans-blue-team/DeepBlueCLI

Detected events

- Suspicious account behavior
  - User creation
  - User added to local/global/universal groups
  - Password guessing (multiple logon failures, one account)
  - Password spraying via failed logon (multiple logon failures, multiple accounts)
  - Password spraying via explicit credentials
  - Bloodhound (admin privileges assigned to the same account with multiple Security IDs)
- Command line/Sysmon/PowerShell auditing
  - Long command lines
  - Regex searches
  - Obfuscated commands
  - PowerShell launched via WMIC or PsExec
  - PowerShell Net.WebClient Downloadstring
  - Compressed/Base64 encoded commands (with automatic decompression/decoding)
  - Unsigned EXEs or DLLs
- Service auditing
  - Suspicious service creation
  - Service creation errors
  - Stopping/starting the Windows Event Log service (potential event log manipulation)
- Mimikatz
  - `lsadump::sam`
- EMET & Applocker Blocks

...and more



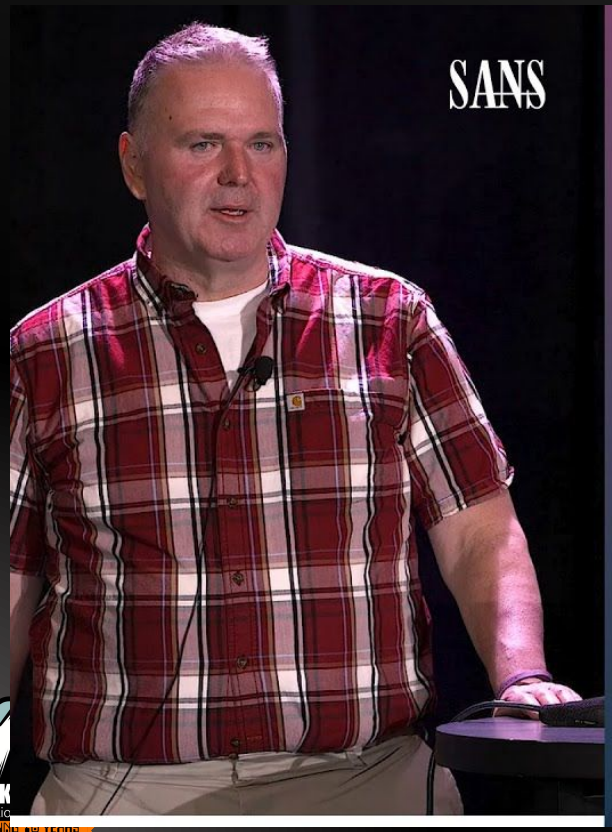
Blue Team Summit

Threat Hunting via Sysmon

- Eric Conrad

Backdoors & Breaches

DeepBlueCLI



Blue Team Summit

Threat Hunting via Sysmon

- Eric Conrad

Backdoors & Breaches

DeepWhiteCLI

DeepWhite

Detective whitelisting using Sysmon event logs.

Parses the Sysmon event logs, grabbing the SHA256 hashes from process creation (event 1), driver load (event 6, sys), and image load (event 7, DLL) events.

VirusTotal and Whitelisting setup

Setting up VirusTotal hash submissions and whitelisting:

The hash checker requires Post-VirusTotal:

- https://github.com/darkoperator/Posh-VirusTotal

It also requires a VirusTotal API key:

- https://www.virustotal.com/en/documentation/public-api/

Then configure your VirusTotal API key:

```
set-VTAPIKey -APIKey <API Key>
```

The script assumes a personal API key, and waits 15 seconds between submissions.

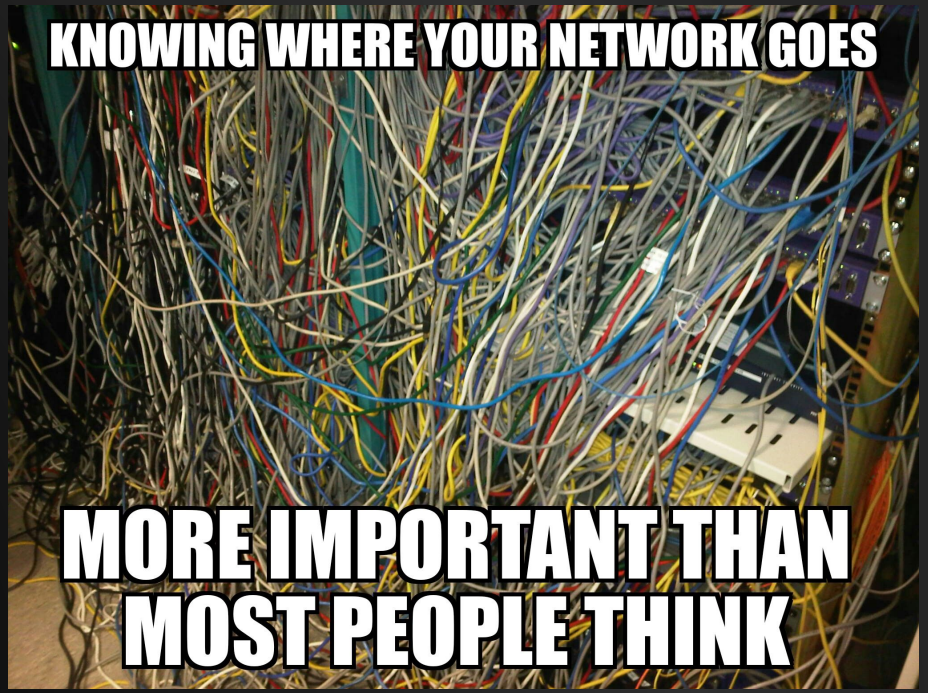
Baseline Whitelisting

```
PS C:\> Get-ChildItem
c:\windows\system32 -Include
'*.exe','*.dll','*.sys','*.com'
-Recurse | Get-FileHash|
Export-Csv -Path whitelist.csv
```

Network

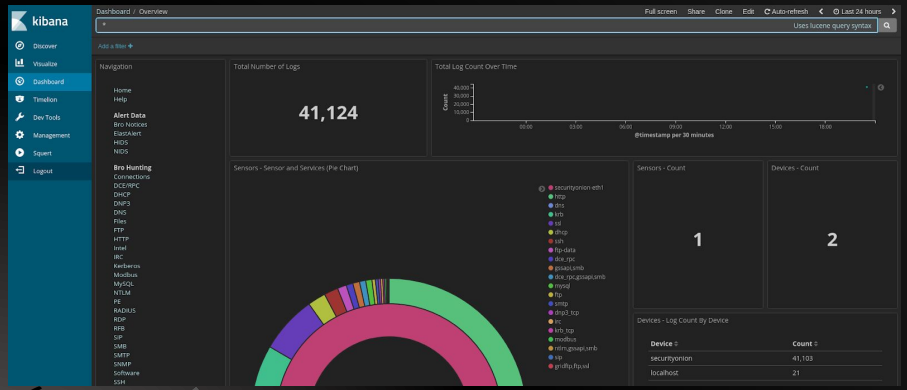
You really need:

- Security Onion
- Suricata
- Bro/Zeek
- RITA
- Access to firewall logs
- Possibly Ntop
- Coffee



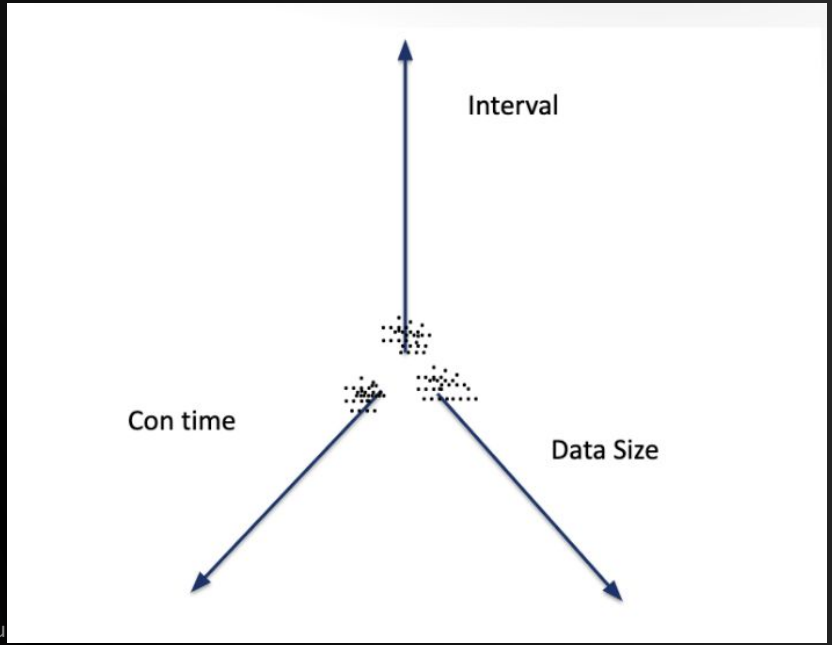
Security Onion

- Security Onion is free and kicks most commercial tools to the curb
- They offer training
- Zeek, Suricata and so much more are included
- Works with RITA!!!



RITA

- You knew this was going to be here



RITA

```
thunt@thunt-one-day:~/lab1$ rita show-long-connections lab1 | head
Source IP,Destination IP,Port:Protocol:Service,Duration
10.55.100.100,65.52.108.225,443:tcp:-,86222.4
10.55.100.107,111.221.29.113,443:tcp:-,86220.1
10.55.100.110,40.77.229.82,443:tcp:-,86160.1
10.55.100.109,65.52.108.233,443:tcp:ssl,72176.1
10.55.100.105,65.52.108.195,443:tcp:ssl,66599
10.55.100.103,131.253.34.243,443:tcp:-,64698.4
10.55.100.104,131.253.34.246,443:tcp:ssl,57413.3
10.55.100.111,111.221.29.114,443:tcp:-,46638.5
10.55.100.108,65.52.108.220,443:tcp:-,44615.2
thunt@thunt-one-day:~/lab1$ _
```

RITA

```
thunt@thunt-one-day:~/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
 Dispersion,Size Dispersion
1,192.168.88.2,165.227.88.15,108858,199,860,230,1,89,53341,108319,0,0,0,0
1,10.55.100.111,165.227.216.194,20054,92,29,52,1,52,7774,20053,0,0,0,0
0.838,10.55.200.10,205.251.194.64,210,308,29398,4,300,70,109,205,0,0,0,0
0.835,10.55.200.11,205.251.197.77,69,308,1197,4,300,70,38,68,0,0,0,0
0.834,192.168.88.2,13.107.5.2,27,198,2,33,12601,73,4,15,0,0,0,0
0.834,10.55.100.111,34.239.169.214,34,704,5,4517,1,156,15,30,0,0,0,0
0.833,10.55.100.106,23.52.161.212,27,940,38031,52,1800,505,19,19,0,0,0,0
0.833,10.55.100.111,23.52.162.184,27,2246,37828,52,1800,467,23,25,0,0,0,0
0.833,10.55.100.100,23.52.161.212,26,797,36042,52,1800,505,16,25,0,0,0,0
thunt@thunt-one-day:~/lab1$
```

Memory Forensics

- Memory forensics is key
  - Volatility
  - Rekall
- Start practicing
- Start with network connections
- Work backwards
- https://www.blackhillsinfosec.com/webcast-windows-memory-forensics/

Command Prompt - rekal -f 504_full_Pivot.dmp

```
[1] 504_full_Pivot.dmp 07:18:15> pslist
------------------------------> pslist()
_EPROCESS          name          pid   ppid  thread_count handle_count session_id wow64    process_create_time
process_exit_time
---------- -------------------- ----- ------ ------------ ------------ ---------- ------ ----------------------- ---
--------------------
0x84f4a7e0 System                  4      0           94          572          - False  2017-04-24 19:21:48Z     -

0x863a3d40 smss.exe              260      4            3           29          - False  2017-04-24 19:21:48Z     -

0x86b089d0 csrss.exe             352    336            9          497          0 False  2017-04-24 19:21:49Z     -

0x86d9e030 msdtc.exe             368    476           12          144          0 False  2017-04-24 19:21:54Z     -

0x86a8d978 wininit.exe           404    336            3           74          0 False  2017-04-24 19:21:49Z     -

0x86cb55b0 services.exe          476    404           11          217          0 False  2017-04-24 19:21:49Z     -

0x86ccd5b0 lsass.exe             484    404            7          606          0 False  2017-04-24 19:21:49Z     -

0x86cbb858 lsm.exe               492    404            9          149          0 False  2017-04-24 19:21:49Z     -
```

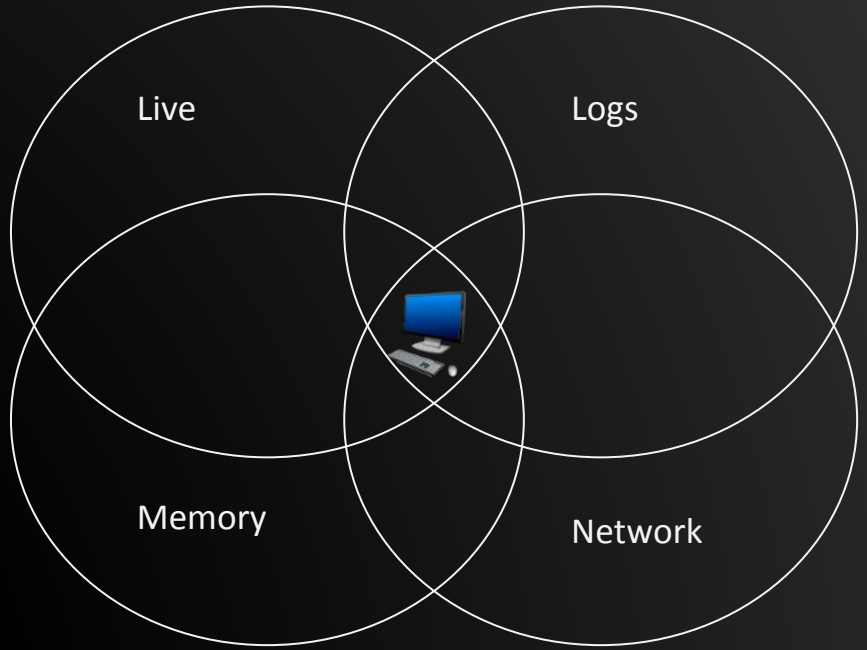
Cheat Sheets!!!

- Soo.. Command line and Powershell logging is kind of important..

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html

- https://zeltser.com/cheat-sheets/
- https://digital-forensics.sans.org/community/cheat-sheets
- https://www.sans.org/blog/4-cheat-sheets-for-malware-analysis/
- https://cheatography.com/tag/ir/
- https://www.malwarearchaeology.com/cheat-sheets

Overlap



WILD WEST HACKIN' FEST

www.wildwesthackinfest.com

Watch Past WWHF Talks on YouTube

BLACK HILLS
Information Security

Backdoors &Breaches

PENETRATION TESTING

RED TEAMING

THREAT HUNTING

WEBCASTS

OPEN-SOURCE TOOLS

BLOGS

bhis.co

AI HUNTER™

Network Threat Hunting Solution

ANALYZE
Network Traffic

IDENTIFY
Compromised Systems

HUNT
Menacing Threats

- BEACONS MODULE
- LONG CONNECTIONS MODULE
- DEEP DIVE MODULE
- ALERTING

acm.re