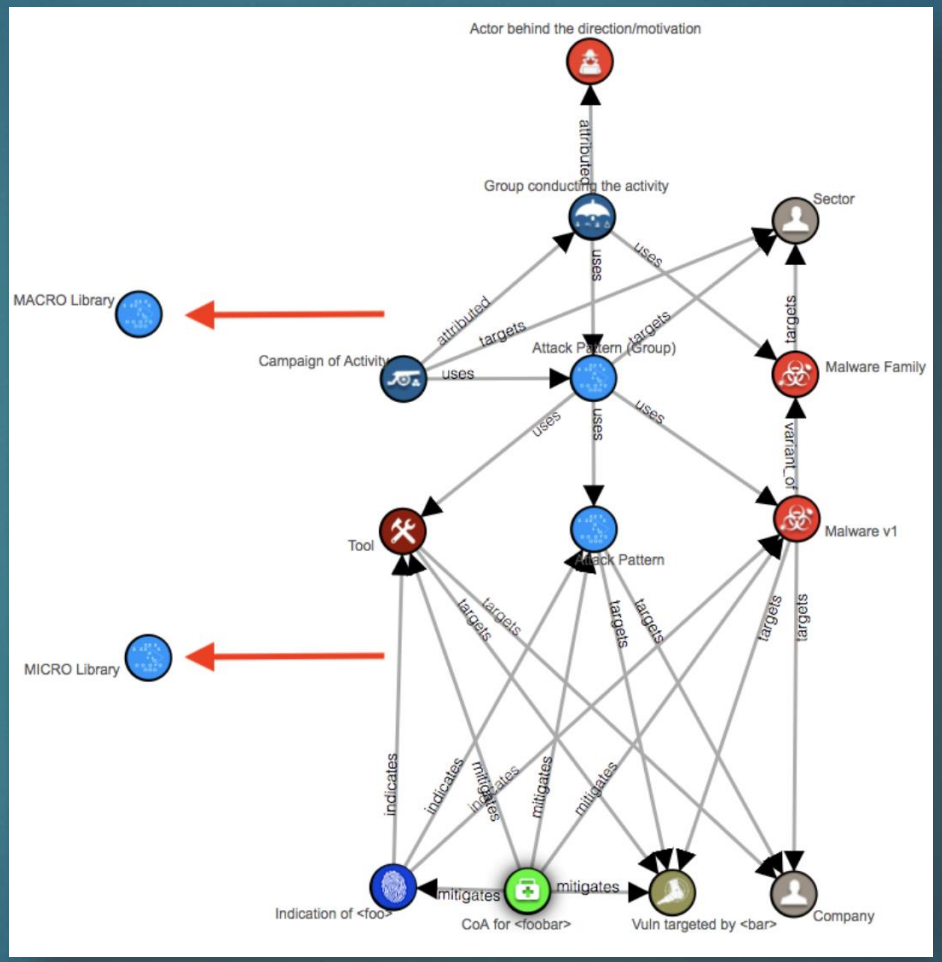
CTI Collaboration

CHRIS O'BRIEN

TLDR;

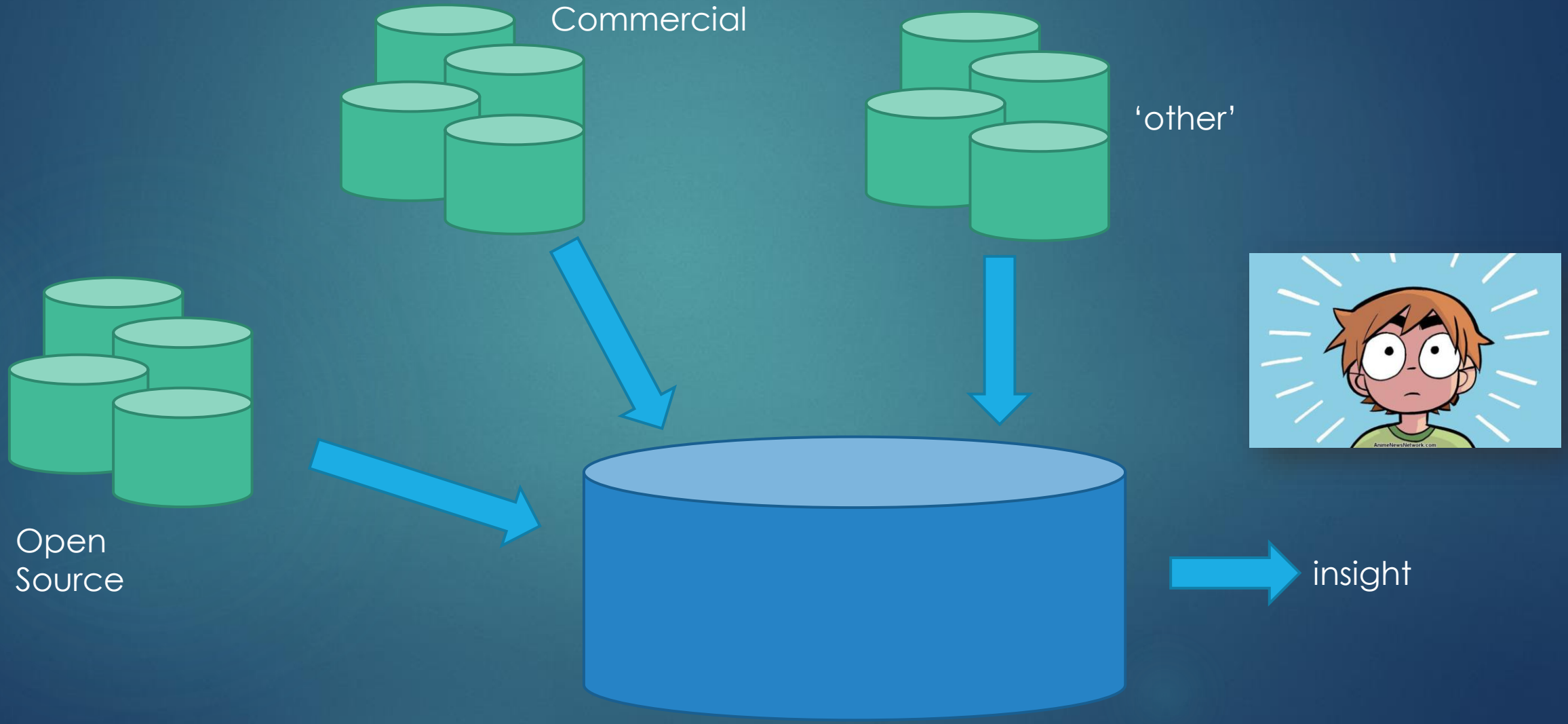
- I love STIX. But…
- Data normalisation kills hollistic intelligence analysis
  - DAG / git-ification of intelligence ‘commits’
  - Need representation of objective and subjective views…
  - …without global data normalisation
- Behavioural Security models require Behavioural Intelligence models
  - Mitre ATT&CK is 1, there should be more
  - Need a way to manage intelligence behavioral models (macro<>micro)
- In order to… provide a means for de-centralised intelligence collaboration

RetCon…



OASIS Borderless / FIRST TC – Dec, 17

Problem 1: Global Data Normalisation



Problem 2: Macro<>Micro

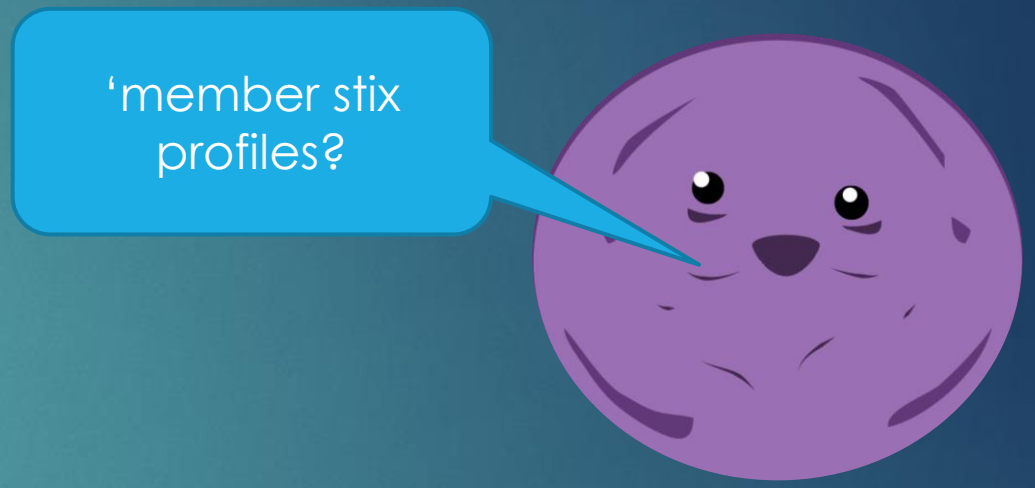
- Requires strong, **agreed**, consistent libraries
  - eg: Mitre ATT&CK
- Contributions are good, including opinions, but alternate viewpoints/realities are not maintained (implied as a meta-layer)
- Implementation often leads to "tagging" mindset – fine, but results in hyperconnectivity
- "Scope" of object is not universal, eg:
  - "Attack Patterns are used to help categorise attacks…", but also…
  - "Attack Patterns can also be more specific…"

Working theory…

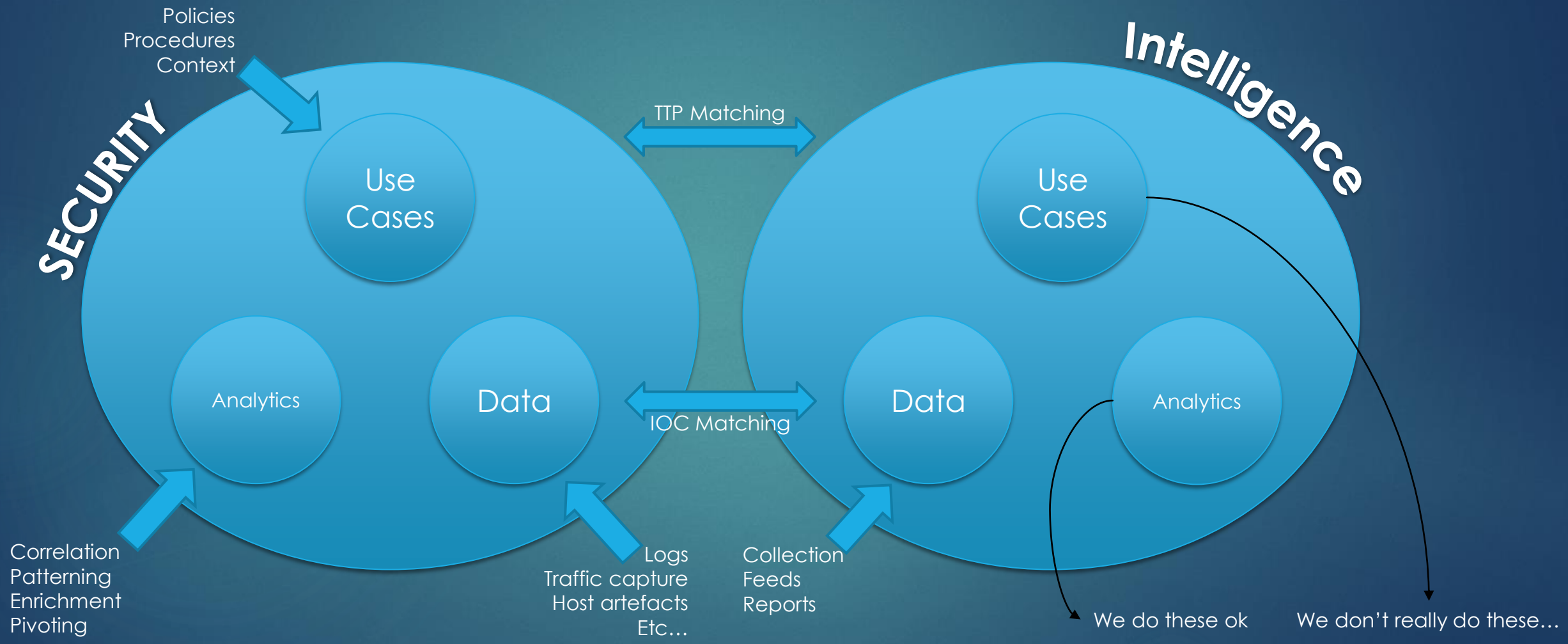
- 1 data model will not rule them all
- Find a way that producers can create what they like, using:
  - **Molecules**: to allow consumers to pivot at a behavioral level
  - **git4intel**: to allow consumers to view intel through their "lens".

Molecules

QUERY FOR BEHAVIOURAL LEVEL INTELLIGENCE



Behavioural Approach



Molecule Schemas (eg: elastic)

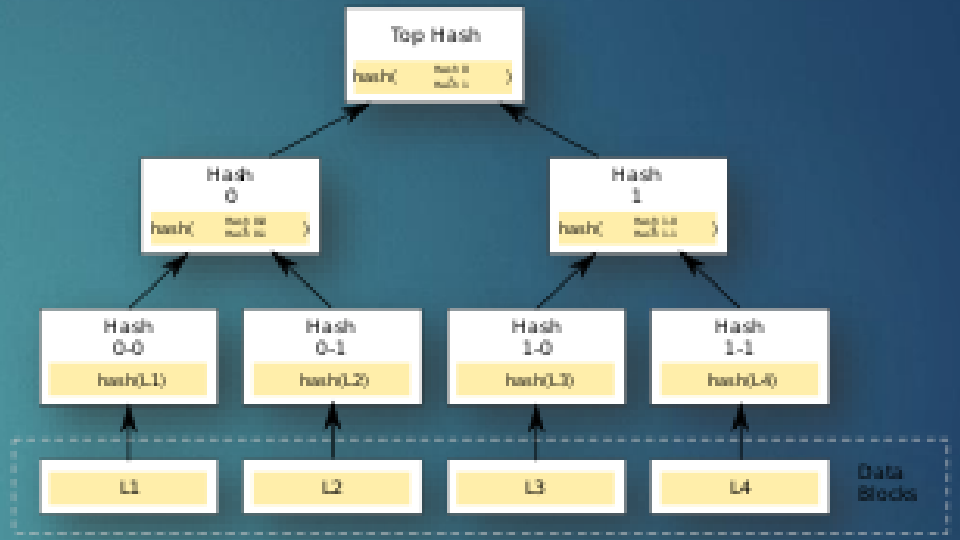
hunt.json

```
{
    "name": "hunt",
    "core": {"bool": {"should": [
        {"bool": {"must": [
            {"match": {"type": "indicator"}}
        ]}},
        {"bool": {"must": [
            {"match": {"type": "relationship"}},
            {"match": {"relationship_type": "indicates"}},
            {"match": {"source_ref": "indicator--"}},
            {"bool": {"should": [
                {"match": {"target_ref": "attack-pattern--"}},
                {"match": {"target_ref": "malware--"}},
                {"match": {"target_ref": "tool--"}}
            ]}}
        ]}}
    ]}},
    "ext": {"bool": {"should": []}}
}
```

- ^^ basic inference (shout-out: OpenCTI)
- >> Complex library graph walk
- Ideally more “programmatic” (shout-out: GraphI)
- Query in a “1-shot” for behavioral concept
- Avoid macro<>micro explosions

mitre.json

```
{
    "name": "mitre",
    "core": {"bool": {"should": [
        {"bool": {"must": [
            {"match": {"type": "attack-pattern"}},
            {"match": {"created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b5
        ]}},
        {"bool": {"should": [
            {"match": {"type": "tool"}},
            {"match": {"type": "malware"}}
        ]}},
        {"bool": {"must": [
            {"match": {"type": "relationship"}},
            {"match": {"relationship_type": "uses"}},
            {"match": {"target_ref": "attack-pattern--"}},
            {"bool": {"should": [
                {"match": {"source_ref": "attack-pattern--"}},
                {"match": {"source_ref": "malware--"}},
                {"match": {"source_ref": "tool--"}}
            ]}}
        ]}},
        {"bool": {"must": [
            {"match": {"type": "relationship"}},
            {"match": {"relationship_type": "uses"}},
            {"match": {"source_ref": "intrusion-set--"}},
            {"bool": {"should": [
                {"match": {"target_ref": "attack-pattern--"}},
                {"match": {"target_ref": "malware--"}},
                {"match": {"target_ref": "tool--"}}
            ]}}
        ]}},
        {"bool": {"must": [
            {"match": {"type": "relationship"}},
            {"match": {"relationship_type": "mitigates"}},
            {"match": {"source_ref": "course-of-action--"}},
            {"bool": {"should": [
                {"match": {"target_ref": "attack-pattern--"}},
                {"match": {"target_ref": "malware--"}},
                {"match": {"target_ref": "tool--"}}
            ]}}
        ]}}
    ]}},
    "ext": {"bool": {"should": [
        {"bool": {"must": [
            {"match": {"type": "intrusion-set"}}
        ]}},
        {"bool": {"must": [
            {"match": {"type": "course-of-action"}}
        ]}}
    ]}}
}
```



git4intel

TREAT INTELLIGENCE AS PROVENANCE-RICH COMMITS TO FORK, BRANCH AND OTHERWISE CREATE CUSTOM VIEWS ON THE SAME DATA.

Given:
- None.

Assert:

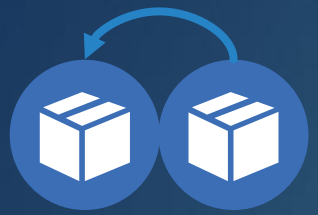
Commit:
aaaaaa
- ISET exists
- Malware used
- Implied: Campaign observed

U/K

Intel equivalent (eg: alias)

Clerical duplicate

aaaaaa



aaaaaa

bbbbbb

Given:

Commit: aaaaaa

Assert:

Commit: bbbbbb

- Indicator of malware exists
- Malware is the same

U/K

aaaaaa

bbbbbb

cccccc

Given:

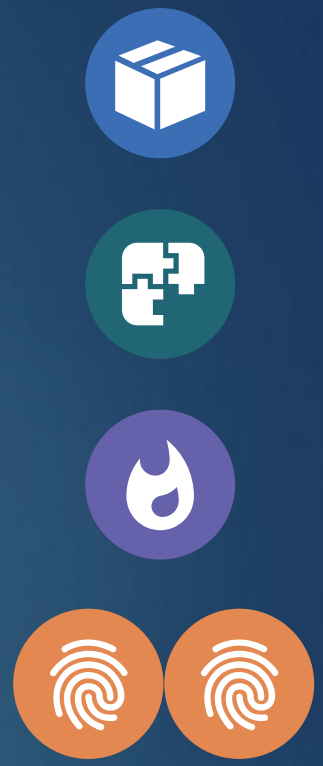
Commit: aaaaaa

Commit: bbbbbb

Assert:

Commit: cccccc

- Indicator of malware exists
- Malware is the same
- Iset is the same (as an alias)
- Campaign identified (timestamp?)



aaaaaa | bbbbbb | cccccc | 111111

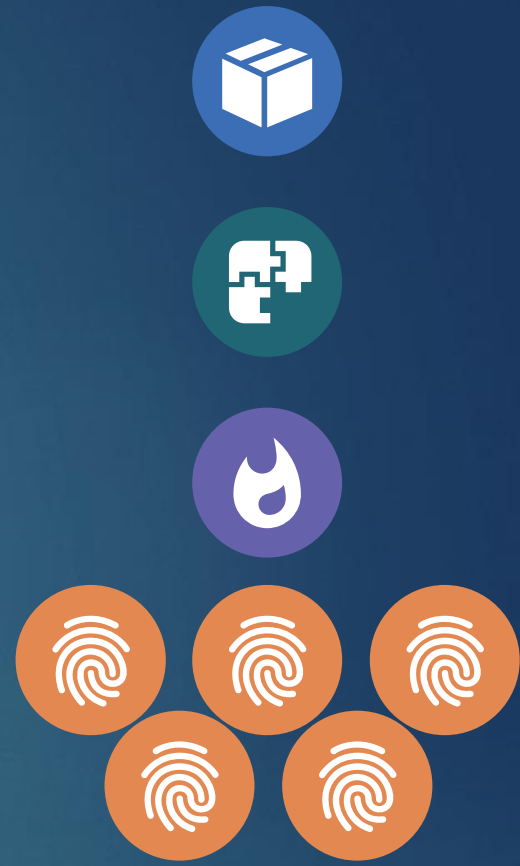
Given:

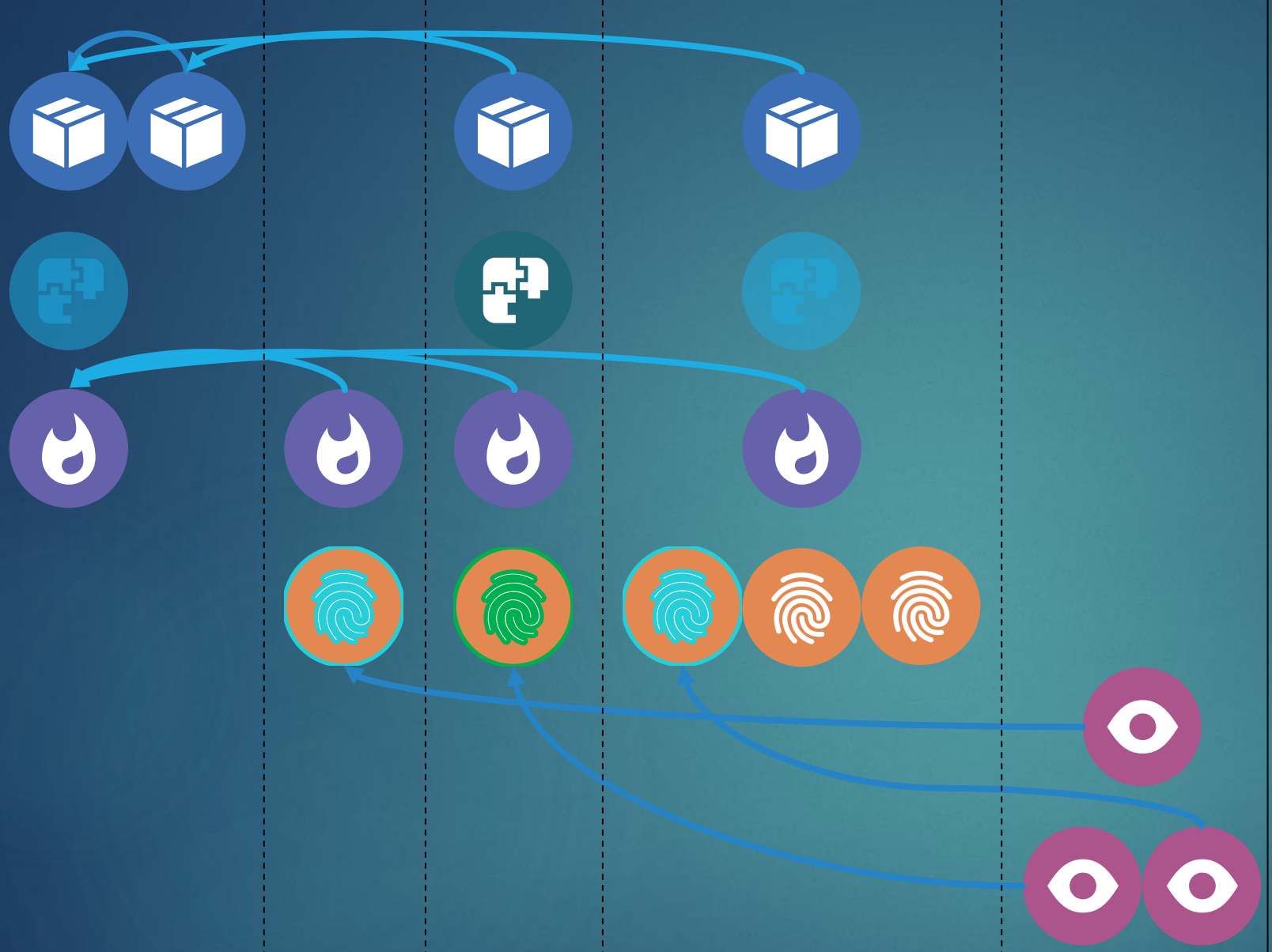
- Commit: aaaaaa
- Commit: bbbbbb
- Commit: cccccc

Assert:

Commit: 111111

- Indicator of malware exists
- Malware is the same
- Iset is the same (as an alias)
- Campaign identified (timestamp?)





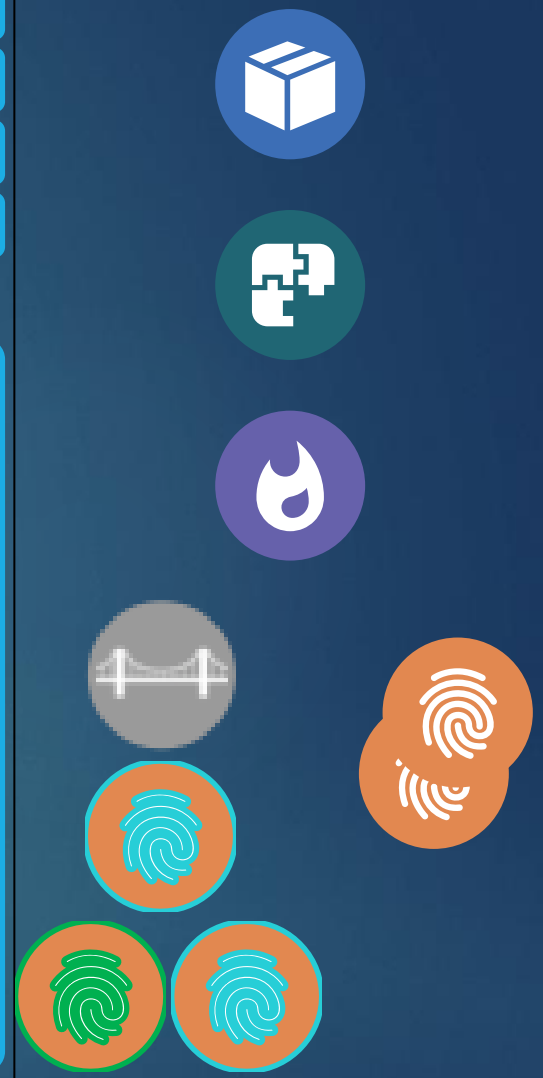
Given:

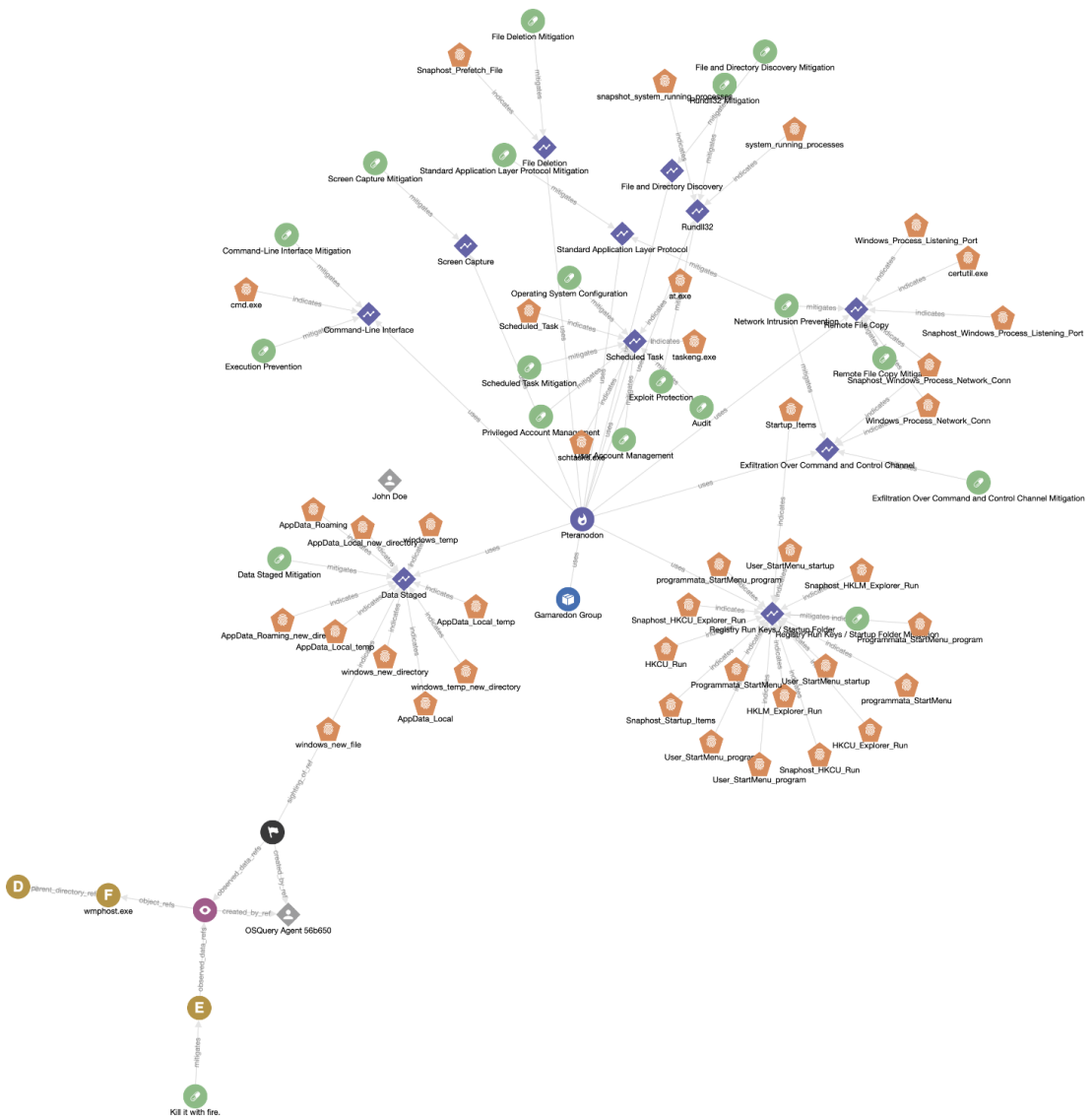
- Commit: aaaaaa
- Commit: bbbbbb
- Commit: cccccc
- Commit: 111111

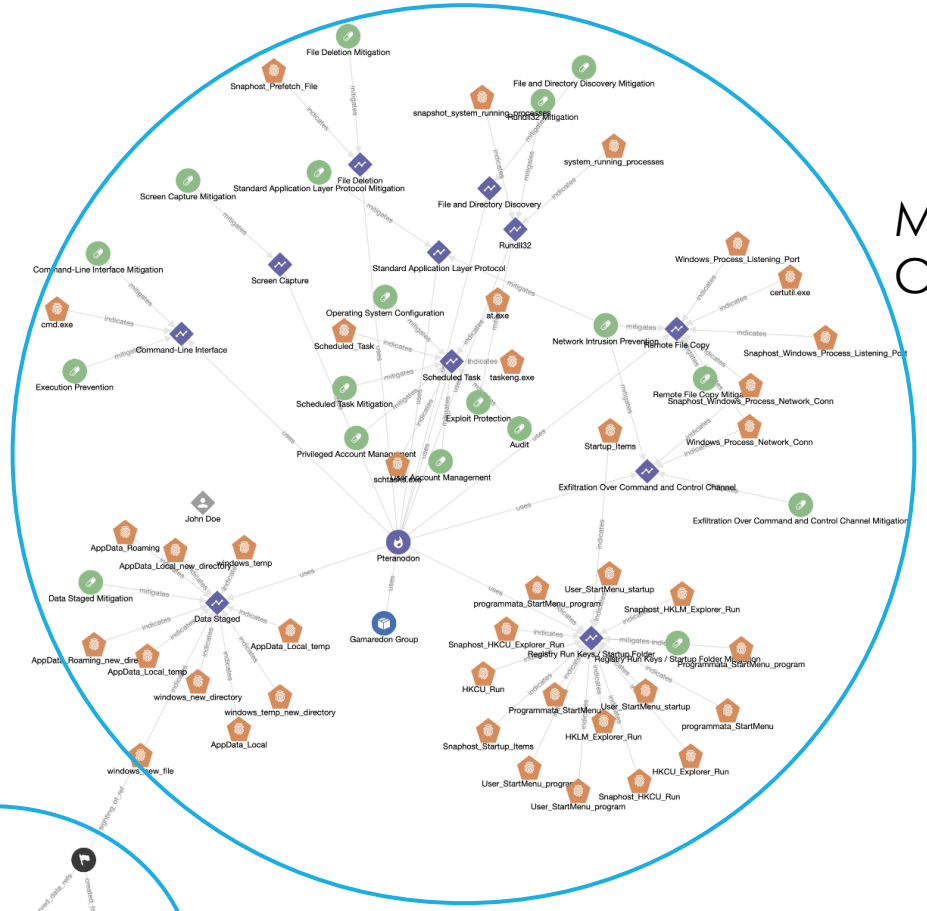
Assert:

Commit: 222222

- IP address likely infrastructure (control of resolution)
- Legit vs Malicious
- Remainder continue malware indicator only

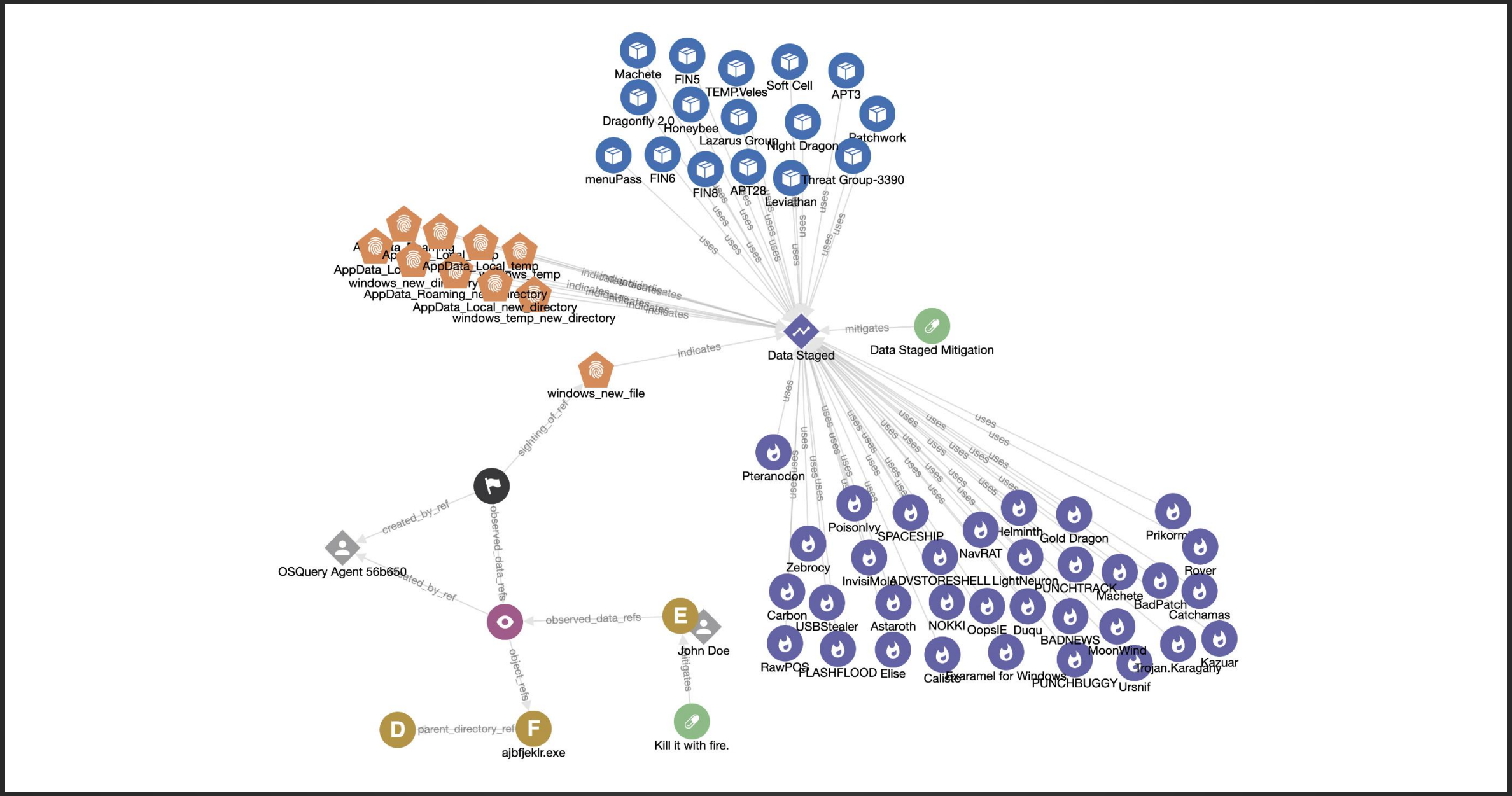



File Deletion Mitigation
Snaphost_Prefetch_File
File and Directory Discovery Mitigation
snapshot_system_running_processes
Forensics Mitigation
system_running_processes
File Deletion
Standard Application Layer Protocol Mitigation
File and Directory Discovery
Screen Capture Mitigation
Rundll32
Command-Line Interface Mitigation
Screen Capture
Standard Application Layer Protocol
Windows_Process_Listening_Port
certutil.exe
Operating System Configuration
at.exe
cmd.exe
Network Intrusion Prevention
Remote File Copy
Snaphost_Windows_Process_Listening_Port
Scheduled_Task
Command-Line Interface
Scheduled Task
taskeng.exe
Execution Prevention
Remote File Copy Mitigation
Snaphost_Windows_Process_Network_Conn
Scheduled Task Mitigation
Exploit Protection
Audit
Startup_Items
Windows_Process_Network_Conn
Privileged Account Management
schtasks.exe
Privileged Account Management
Exfiltration Over Command and Control Channel
Exfiltration Over Command and Control Channel Mitigation
John Doe
AppData_Roaming
AppData_Local_new_directory
windows_temp
Pteranodon
Data Staged Mitigation
Data Staged
Gamaredon Group
User_StartMenu_startup
programmata_StartMenu_program
Snaphost_HKLM_Explorer_Run
Snaphost_HKCU_Explorer_Run
Registry Run Keys / Startup Folder
Registry Run Keys / Startup Folder Mitigation
Programmata_StartMenu_program
AppData_Roaming_new_directory
AppData_Local_temp
AppData_Local_temp
HKCU_Run
Programmata_StartMenu
User_StartMenu_startup
windows_new_directory
windows_temp_new_directory
HKLM_Explorer_Run
programmata_StartMenu
AppData_Local
Snaphost_Startup_Items
HKCU_Explorer_Run
User_StartMenu_program
Snaphost_HKCU_Run
User_StartMenu_program
windows_new_file
sighting_of_ref
observed_data_refs
created_by_ref
parent_directory_ref
object_refs
wmphost.exe
OSQuery Agent 56b650
observed_data_refs
mitigates
Kill it with fire.



Multi-commit CTI space

Incident Response


Machete
FIN5
TEMP.Veles
Soft Cell
APT3
Dragonfly 2.0
Honeybee
Lazarus Group
Night Dragon
Patchwork
menuPass
FIN6
FIN8
APT28
Leviathan
Threat Group-3390
AppData_Local_temp
windows_temp
AppData_Local_new_directory
windows_temp_new_directory
indicates
Data Staged
mitigates
Data Staged Mitigation
windows_new_file
sighting_of_ref
created_by_ref
observed_data_refs
OSQuery Agent 56b650
E
John Doe
mitigates
object_refs
D
parent_directory_ref
F
ajbfjeklr.exe
Kill it with fire.
uses
Pteranodon
PoisonIvy
SPACESHIP
NavRAT
Helminth
Gold Dragon
Prikormka
Zebrocy
InvisiMole
ADVSTORESHELL
LightNeuron
PUNCHTRACK
Machete
Rover
BadPatch
Catchamas
Carbon
USBStealer
Astaroth
NOKKI
OopsIE
Duqu
BADNEWS
MoonWind
Kazuar
RawPOS
FLASHFLOOD
Elise
Calisto
Exaramel for Windows
PUNCHBUGGY
Ursnif
Trojan.Karagany

Conclusion

- Still <3 stix
- Data models are never perfect => will never be universal
- Behavioral Intelligence templates (like inference, molecules, etc) can provide an alternative – let consumers search by **use case** rather than by data
- Leveraging provenance to support git-like data management can provide a means for users to choose their own adventure – removing the need for universal data normalisation.