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...
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

‘member stix profiles?
Behavioural Approach

Use Cases

Data

Analytics

Correlation
Patterning
Enrichment
Pivoting

Policies
Procedures
Context

Logs
Traffic capture
Host artefacts
Etc...

IOC Matching

TTP Matching

Use Cases

Data

Analytics

Collection
Feeds
Reports

Intelligence

We do these ok

We don’t really do these…
Molecule Schemas (eg: elastic)

- ^^ basic inference (shout-out: OpenCTI)
- >> Complex library graph walk
- Ideally more “programmatic” (shout-out: Grapl)
- Query in a “1-shot” for behavioral concept
- Avoid macro<>micro explosions
git4intel

TREAT INTELLIGENCE AS PROVENANCE-RICH COMMITS TO FORK, BRANCH AND OTHERWISE CREATE CUSTOM VIEWS ON THE SAME DATA.
Given:
- None.

Assert:
- ISET exists
- Malware used
- Implied: Campaign observed

Intel equivalent (e.g. alias)
Clerical duplicate
Given:
Commit: aaaaaa

Assert:
Commit: bbbbbbb
- Indicator of malware exists
- Malware is the same
Given:

- None.

Assert:

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

Commit: aaaaaa
Commit: bbbbbbb
Commit: ccccccc
Given:

- Commit: aaaaaa
- Commit: bbbbbbb
- 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: bbbbbbb
- Commit: ccccccc
- Commit: 111111

Assert:
- Commit: 222222
  - IP address likely infrastructure (control of resolution)
  - Legit vs Malicious
  - Remainder continue malware indicator only
Multi-commit CTI space

Incident Response
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.