EVALUATE OR DIE TRYING

A METHODOLOGY FOR QUALITATIVE EVALUATION OF CYBER THREAT INTELLIGENCE FEEDS
Agenda

Problem Statement

Previous Work

Our Approach

Metrics

So What?
Problem Statement
Evolution?
More organizations are consuming CTI, especially in the form of finalized intelligence reports, and integrating them into their defensive mechanisms. **Operationalizing narrative-based intelligence reports**—reports that describe in detail a series of events related to an intrusion or incident—is time-consuming for CTI analysts. A lack of automation for these reports makes them especially time-consuming. CTI teams need to ensure that they are properly staffed and allocating enough time to make the best use of this type of reporting.

The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey
Threat Intelligence Fatigue

• Organizations tend to obtain as much information as possible

• Sources not meeting **intelligence** and **production** requirements

• Customer cannot judge the **quality** of an intel feed

• Unknown business value.

• How to justify expenditures for intelligence sources?
Previous Work
Previous Work

Measuring the IQ of your Threat Intelligence
Alexandre Pinto, Kyle Maxwell, DEFCON 22, August 2014

Data-Driven Threat Intelligence:
Useful Methods and Measurements for Handling Indicators
Alexandre Pinto, Alexandre Sieira, FIRST Conference 2015, June 2015

Evaluating Threat Intelligence Feeds
Paweł Pawlinski, Andrew Kompanek, FIRST Technical Colloquium for Threat Intelligence Munich, 2016

This is still a must. Our work is NOT a replacement, but should co-exist with earlier work.
Our Approach
Our Approach

- We use STIX 2.0 as common format for comparison
- Ingest native STIX 2.0 feeds
- Convert existing STIX 1.2 feed into STIX 2.0
- Convert source specific JSON into STIX 2.0
- Store STIX 2.0 data in PostgreSQL DB
- Use Jupyter notebook for analysis
• We are looking at the feed of decent size (difficult to eye-ball)

• The feeds are updated daily, append-only.

• Mix of open and commercial sources

• We focus on STIX 2.0 objects (one feed contained STIX 2.1 entities)

• Convert existing STIX 1.2 / JSON feeds into STIX 2.0 with best effort
Metrics
Objects & observables
Object Type Variability

- Do these object types align with my needs?
- Is the feed balanced or is it heavily skewed to one particular object type?
- Are there custom STIX2 objects that might cause ingestion issues?
Object Type Variability

- Do these object types align with my needs?
- Is the feed balanced or is it heavily skewed to one particular object type?
- Are there custom STIX2 objects that might cause ingestion issues?
Object Type Variability

Source C

Source F

Objects per type

Objects per type (log scale)
Do these observable types align with my needs?
Is feed balanced or is it heavily skewed to one particular observable type?
Observables Variability

Source C

No Observables

Source D

1 observable type + path pairs

- Do these observable types align with my needs?
- Is feed balanced or is it heavily skewed to one particular observable type?
Timeframe & Gaps

• Does the source contain enough historical data?
• Are there significant gaps in the dataset?
• Is daily data influx consistent over long period of time?
Timeframe & Gaps

- Does the source contain enough historical data?
- Are there significant gaps in the dataset?
- Is daily data influx consistent over long period of time?
Influx

- What is the daily average for the last 30 days?
- Does the feed contain spikes that can cause performance issues during ingestion?
- Is the feed balanced across object types or is it skewed to one particular object type?
• What is the daily average for the last 30 days?
• Does the feed contain spikes that can cause performance issues during ingestion?
• Is the feed balanced across object types or is it skewed to one particular object type?
2.4.1 Properties

### Common Properties
- type, id, created, created_ref, created_by_ref, modified, revoked, labels, external_references, object_marking_refs, granular_markings

### Identity Specific Properties
- name, description, identity_class, sectors, contact_information

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type (required)</td>
<td>string</td>
<td>The value of this property MUST be identity.</td>
</tr>
<tr>
<td>labels (optional)</td>
<td>list of string</td>
<td>The list of roles that this identity performs e.g., CEO, Domain Administrator, Doctors, Hospital, or Retailer. No open vocabulary is yet defined for this property.</td>
</tr>
<tr>
<td>name (required)</td>
<td>string</td>
<td>The name of this identity. When referring to a specific entity (e.g., an individual or organization), this property SHOULD contain the canonical name of the specific entity.</td>
</tr>
<tr>
<td>description (optional)</td>
<td>string</td>
<td>A description that provides more details and context about the identity, potentially including its purpose and its key characteristics.</td>
</tr>
<tr>
<td>identity_class (required)</td>
<td>open-vocab</td>
<td>The type of entity that this identity describes, e.g., an individual or organization. This is an open vocabulary and the values SHOULD come from the identity-class open vocabulary.</td>
</tr>
<tr>
<td>sectors (optional)</td>
<td>list of open-vocab</td>
<td>The list of Industry sectors that this identity belongs to.</td>
</tr>
</tbody>
</table>
Fullness

- Does the source leverage optional fields or does it provide minimum context only?
- Does the source implement custom fields?
Relationships
Relationship by Type

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship type or, as with open vocabularies, user-defined names.

<table>
<thead>
<tr>
<th>Embedded Relationships</th>
</tr>
</thead>
<tbody>
<tr>
<td>created_by_ref</td>
</tr>
<tr>
<td>object_marking.refs</td>
</tr>
</tbody>
</table>

| identifier (of type identity)           |
| identifier (of type marking-definition) |

<table>
<thead>
<tr>
<th>Common Relationships</th>
</tr>
</thead>
<tbody>
<tr>
<td>duplicate-of, derived-from, related-to</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
<th>Relationship Type</th>
<th>Target</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reverse Relationships</th>
</tr>
</thead>
<tbody>
<tr>
<td>attack-pattern, campaign, intrusion-set, malware, threat-actor, tool</td>
</tr>
</tbody>
</table>

| targets | vulnerability | See forward relationship for definition. |

STIX™ Version 2.0. Part 2: STIX Objects
https://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part2-stix-objects.html
Relationship by Type

- Does the source use custom relations? Hint at unconventional data model.
- Custom relation types might also cause integration during ingestion.
Does the dataset have objects with unreasonable number of outgoing relations?
- This might be a symptom of a poor data model and might cause issues during ingestion.
Does the dataset have objects with unreasonable number of outgoing relations?
• This might be a symptom of a poor data model and might cause issues during ingestion.
Does the dataset have objects with unreasonable number of outgoing relations?
- This might be a symptom of a poor data model and might cause issues during ingestion.
Outgoing Relationship Between Objects

• How connected is the dataset?
• What data model the dataset has?
Content
No. of Labels per Object Type

- How well is data labeled?
Quality of the content: labels vs description

Source F - No. of Label per Object Type

Source F – Description Length per Object Type

Source F

- Reports: not having any description length, but labeled on average with 2.55 labels
- CoA: an average description length of 1978 chars (with no variance), but no label?
Metrics - Full List

- Object types
- Observable types
- Time frame & gaps
- Objects per day per type
- Fullness
- Relationships by type
- No. of outgoing relationships
- Outgoing relationships between various object types
- Number of incoming relationships per target object type
- Incoming relationships between various object types
- No. of hanging or detached relationships
- Description length per object type
- Number of labels per object type
- Objects per TLP
- Unique and re-used observables
- Observables overlap between feeds
- Relevancy / Proximity
# Metrics - Example

<table>
<thead>
<tr>
<th>Metric</th>
<th>Weighting</th>
<th>Source A Points</th>
<th>Source A Score</th>
<th>Source B Points</th>
<th>Source B Score</th>
<th>Source C Points</th>
<th>Source C Score</th>
<th>Source D Points</th>
<th>Source D Score</th>
<th>Source E Points</th>
<th>Source E Score</th>
<th>Source F Points</th>
<th>Source F Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity Variability</td>
<td>1,50</td>
<td>5</td>
<td>7,5</td>
<td>1</td>
<td>1,5</td>
<td>1</td>
<td>1,5</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>4,5</td>
<td>5</td>
<td>7,5</td>
</tr>
<tr>
<td>Observables Variability</td>
<td>1,20</td>
<td>4</td>
<td>4,8</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1,2</td>
<td>4</td>
<td>4,8</td>
</tr>
<tr>
<td>Time Frame &amp; Gaps</td>
<td>1,10</td>
<td>2</td>
<td>2,2</td>
<td>2</td>
<td>2,2</td>
<td>5</td>
<td>5,5</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>4,4</td>
<td>3</td>
<td>3,3</td>
</tr>
<tr>
<td>Influx per Day</td>
<td>1,00</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Entity Thickness / Completeness</td>
<td>1,20</td>
<td>3</td>
<td>3,6</td>
<td>1</td>
<td>1,2</td>
<td>1</td>
<td>1,2</td>
<td>2</td>
<td>6</td>
<td>2</td>
<td>2,4</td>
<td>2</td>
<td>2,4</td>
</tr>
<tr>
<td>Relationship by Type</td>
<td>1,10</td>
<td>4</td>
<td>4,4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1,1</td>
<td>2</td>
<td>2,2</td>
</tr>
<tr>
<td>No. of Outgoing Relationship</td>
<td>1,00</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Proximity</td>
<td>1,50</td>
<td>1</td>
<td>1,5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1,5</td>
<td>1</td>
<td>1,5</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>31</strong></td>
<td><strong>12,9</strong></td>
<td><strong>10,2</strong></td>
<td><strong>18</strong></td>
<td><strong>19,1</strong></td>
<td><strong>24,7</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Weighting**

- **Source A**
- **Source B**
- **Source C**
- **Source D**
- **Source E**
- **Source F**
Observations & Lessons Learned

• “Results produced by the stix2-elevator are not for production purposes”
  • python libraries used for STIX2 transformation require a lot of hand holding

• Some feeds can not be easily converted to STIX2.0 because of feed / spec limitations:
  • UUID4-only IDs
  • Reports must have `object_refs` field set
  • Indicators must have a pattern

• There are few STIX2.0 sources available (for now), feed providers are taking their time.

• Feed evaluation is a multi-step process of analyzing feed characteristics from intelligence requirements perspective.
So What?
Situation Today

Source A  
no structure

Vendor B  
poor structure

Vendor C  
Intel “hidden” as unstructured data in reports

Consumer Profile

Super Bank Inc.  
Russia  
Sector: Finance

FlawedAmmyy  
FastCash

RDP

VNC
Proximity - Source X

Super Bank Inc.
Sector: Finance
Russia

FlawedAmmyy
FastCash

RDP
VNC

Intelligence provided by source X
Proximity - Source Y

Consumer Profile
- Super Bank Inc.
- Russia
- Sector: Finance
- FlawedAmmyy
- FastCash
- RDP
- VNC

Intelligence provided by source Y
Relevancy - Source A

### Relevant malware

**Malware names:** njrnt, shamoon, loki, lokibot, gandcrab

<table>
<thead>
<tr>
<th>Object type</th>
<th>Objects matched</th>
<th>Objects of this type</th>
<th>% of objects of this type</th>
</tr>
</thead>
<tbody>
<tr>
<td>attack-pattern</td>
<td>48</td>
<td>8395</td>
<td>0.751%</td>
</tr>
<tr>
<td>campaign</td>
<td>22</td>
<td>1119</td>
<td>1.968%</td>
</tr>
<tr>
<td>course-of-action</td>
<td>5</td>
<td>855</td>
<td>0.585%</td>
</tr>
<tr>
<td>identity</td>
<td>6</td>
<td>2028</td>
<td>0.296%</td>
</tr>
<tr>
<td>indicator</td>
<td>59</td>
<td>16442</td>
<td>0.359%</td>
</tr>
<tr>
<td>intrusion-set</td>
<td>3</td>
<td>461</td>
<td>0.851%</td>
</tr>
<tr>
<td>malware</td>
<td>114</td>
<td>3927</td>
<td>2.903%</td>
</tr>
<tr>
<td>report</td>
<td>90</td>
<td>3613</td>
<td>2.491%</td>
</tr>
<tr>
<td>threat-actor</td>
<td>1</td>
<td>304</td>
<td>0.329%</td>
</tr>
<tr>
<td>vulnerability</td>
<td>2</td>
<td>5478</td>
<td>0.037%</td>
</tr>
</tbody>
</table>

### Relevant industry sectors

- **Industry sector:** energy
  - Object type: identity
  - Objects matched: 84
  - Objects of this type: 2028
  - % of objects of this type: 4.142%

- **Industry sector:** government
  - No matches

- **Industry sector:** financial-services
  - Object type: identity
  - Objects matched: 320
  - Objects of this type: 2028
  - % of objects of this type: 15.779%

### Relevant CVEs

- **CVEs:** CVE-2017-11882, CVE-2017-0199, CVE-2018-15982

<table>
<thead>
<tr>
<th>Object type</th>
<th>Objects matched</th>
<th>Objects of this type</th>
<th>% of objects of this type</th>
</tr>
</thead>
<tbody>
<tr>
<td>attack-pattern</td>
<td>76</td>
<td>8395</td>
<td>1.188%</td>
</tr>
<tr>
<td>campaign</td>
<td>15</td>
<td>1119</td>
<td>1.340%</td>
</tr>
<tr>
<td>indicator</td>
<td>47</td>
<td>16442</td>
<td>0.286%</td>
</tr>
<tr>
<td>malware</td>
<td>18</td>
<td>3927</td>
<td>0.458%</td>
</tr>
<tr>
<td>report</td>
<td>62</td>
<td>3613</td>
<td>1.716%</td>
</tr>
<tr>
<td>tool</td>
<td>1</td>
<td>369</td>
<td>0.271%</td>
</tr>
<tr>
<td>vulnerability</td>
<td>11</td>
<td>5478</td>
<td>0.201%</td>
</tr>
</tbody>
</table>
Takeaways

• Consumers must understand and document intelligence & production requirements

• Measure and differentiate between good / bad STIX

• Calculate Proximity

• Leverage the power of intelligence consumers to influence feed providers

• Intelligence provider to improve their feed quality
Learn More / Challenge Us

Sergey Polzunov
sergey@polzunov.com
https://www.linkedin.com/in/polzunov
https://github.com/traut

Jörg Abraham
https://www.linkedin.com/in/joergabraham
@mod_tastic