QUALITY OVER QUANTITY

DETERMINING YOUR CTI DETECTION EFFICACY

David J. Bianco
Principal Engineer, Cybersecurity
Target Corporation
@DavidJBianco
I’d like you to review and identify gaps in what we know about our high priority threat actors going into peak [retail season].

Yeah, I’d like that, too.  
But how…?
TRANSLATION INTO ACTION ITEMS

• Identify our high priority threat actors
• Figure out what we know about each (and how/where to find that info)
• Develop CTI evaluation criteria
• Evaluate and perform gap analysis
DATA COLLECTION & PROCESSING

IOCs
- Dump
- Clean
- Merge
- Visualize

TTPs
- Extract
CTI EVALUATION CRITERIA

• Do we know the adversary’s repeated behaviors?
• How volatile are our IOCs?
• In which lifecycle phase(s) could the adversary operate with impunity?
• Is our intel recent enough to be useful, but with enough history to provide context?
• Where should we concentrate or improve our collection efforts?
Assigning the IOCs and TTPs to phases in MITRE’s ATT&CK™ lifecycle model allows us to see “where” in the lifecycle we know the most.

Source: attack.mitre.org
Most of our CTI centers around the attacker’s process for gaining a foothold in the environment.

We know little about what happens before or after.
Assigning IOCs to the appropriate Pyramid level helps describe their potential volatility and replaceability.

Put another way, we want to maximize our ability to increase the adversary’s cost of action against us.

Source: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
We’re doing pretty well covering most of the Pyramid.

Looks like we need more info about their toolset, though.
Plotting the lifecycle phase vs. Pyramid level can reveal not only current strengths, but also opportunities for improvement.
Box plot of IOC age reveals your balance between currency and history.

"Banding" on the left reveals patterns of collection.
Breaking down the ages by lifecycle phase gives more info about how current we are for each.
Analyzing it by Pyramid level is also useful in comparing IOC ages to volatility. The lower the level, the fresher your IOCs need to be.
TTPS BY TACTIC

Mapping the known TTPs to the ATT&CK Enterprise Matrix quickly shows strengths and weaknesses.

White doesn’t imply a gap. Maybe the actor doesn’t do that thing.

I’d like to find something better.
## Key Challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>What we did</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTI data in multiple repositories</td>
<td>• Developed custom extraction for each and merging/deduplication logic</td>
</tr>
<tr>
<td></td>
<td>• Manual review of priority actor wiki pages</td>
</tr>
<tr>
<td>Data tracked by different repos is inconsistent, sometimes even when it</td>
<td>• Analyzed using estimates and approximations when necessary</td>
</tr>
<tr>
<td>looks the same (e.g., timestamps mean different things)</td>
<td>• Custom merging/deduplication logic</td>
</tr>
<tr>
<td>Converting a one-time analysis into a repeatable, automatable process</td>
<td>• Captured code, documentation and graphs in a Jupyter Notebook</td>
</tr>
<tr>
<td></td>
<td>• Work is still ongoing...</td>
</tr>
</tbody>
</table>
TAKEAWAYS

• Start by identifying your key threat actors
• Where is all your data stored and what does it mean?
• Extract, clean, merge & deduplicate (this is most of the work)
• Map IOCs & TTPs to your favorite lifecycle model and to the Pyramid of Pain
• Visualize to identify gaps
• Automate this process and run it regularly to help keep yourself on track with actionable CTI
I have a question and/or wish to make a short speech...

David J. Bianco
@DavidJBianco