Operationalizing Threat Intelligence

Justin Hall
Director, Security Services

cbts | On a cbts company

Good afternoon! I'm Justin.

Director,
Security Services

Cofounder

Husband
Dad
Lucky Dude

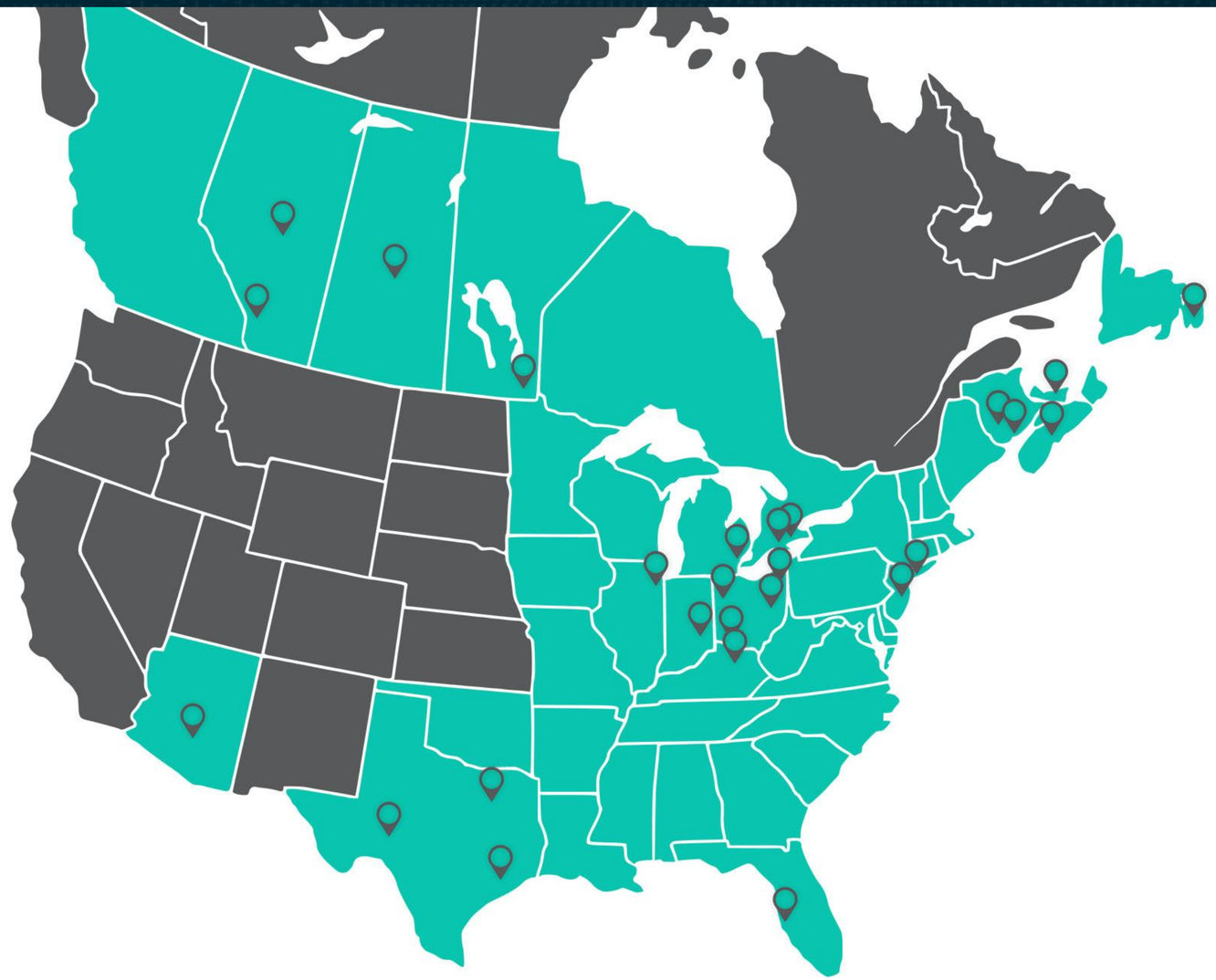
Locations

United States

- Cleveland, OH
- Columbus, OH
- Cincinnati, OH
- Detroit, MI
- Louisville, KY
- Indianapolis, IN
- Dallas, TX
- Phoenix, AZ
- Houston, TX
- Addison, TX
- Chicago, IL
- Tampa, FL
- Mayfield Heights, OH
- Manhattan, NY
- Edison, NJ

Canada & U.K.

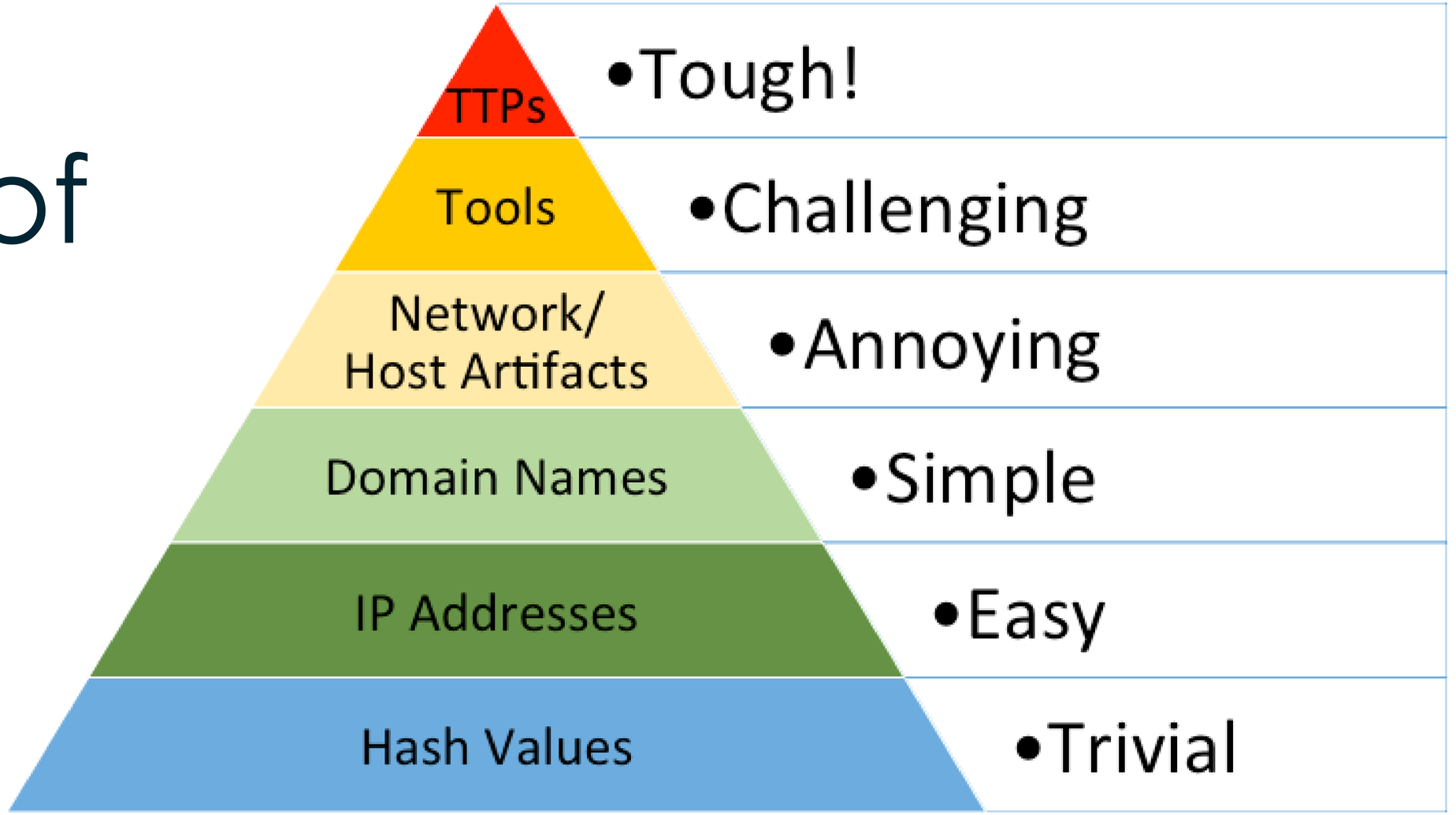
- Calgary, AB
- Edmonton, AB
- Saskatchewan, SK
- Winnipeg, MB
- Cambridge, ON
- Thornhill, ON
- Fredericton, NB
- Saint John, NB
- Halifax, NS
- Saint John's, NL
- Weybridge Surrey, UK



"…evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard…"

source: https://www.gartner.com/doc/2487216/definition-threat-intelligence

Bianco's Pyramid of Pain

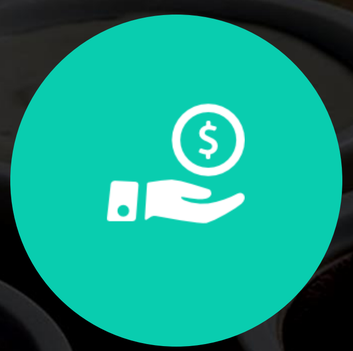


http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Sources

Internal Analysis

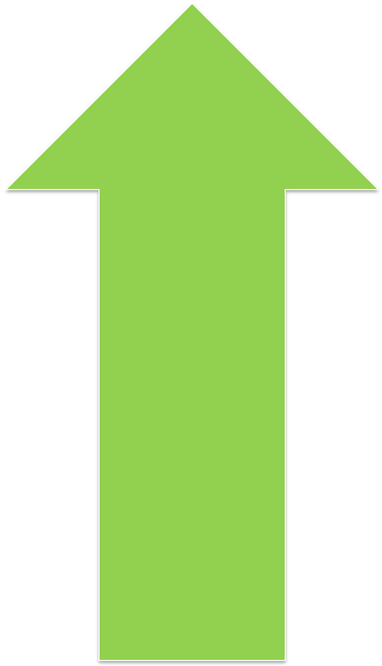
ISAC/ Community



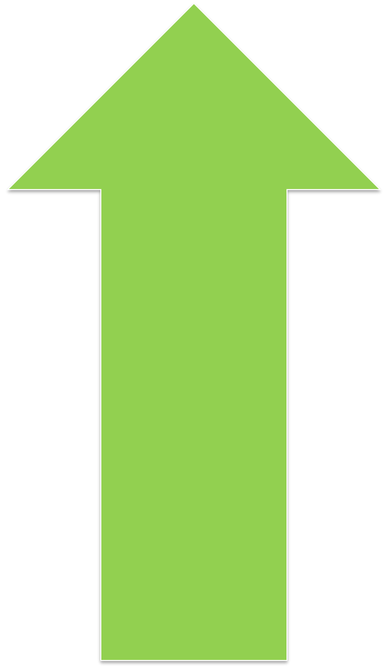
Paid Feeds

Platform

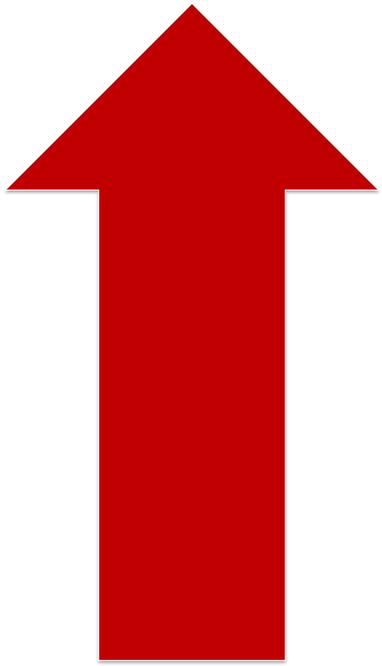
Internal Analysis



High Confidence



High Relevancy



High Cost

ISAC/
Community

Low
Confidence

Moderate
Relevancy

Low
Cost

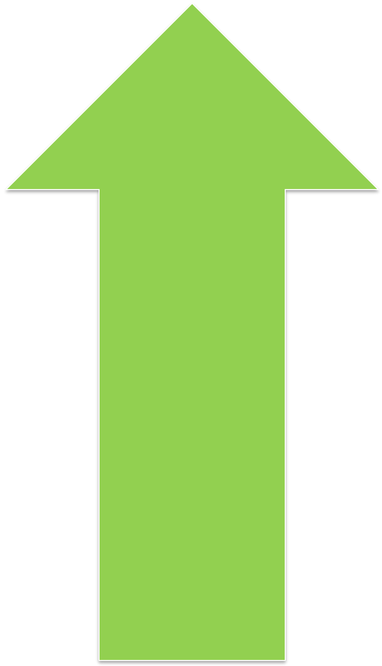
Paid Feeds

Moderate Confidence

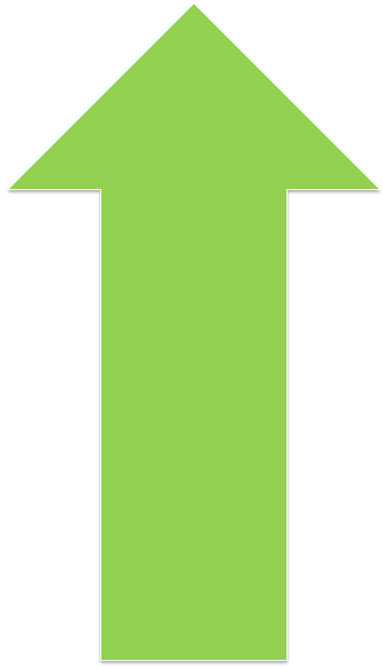
Low Relevancy

Moderate Cost

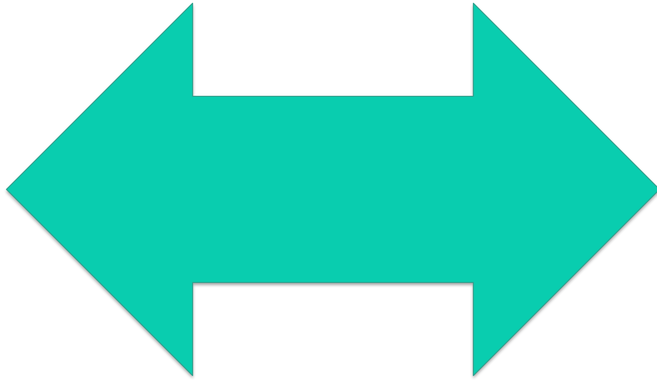
Platform



High Confidence



High Relevancy

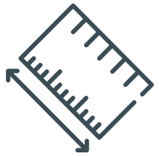


Moderate Cost

Measurement is key!

For each source…

What's the average time from deployment of a signature to detection of a true positive?



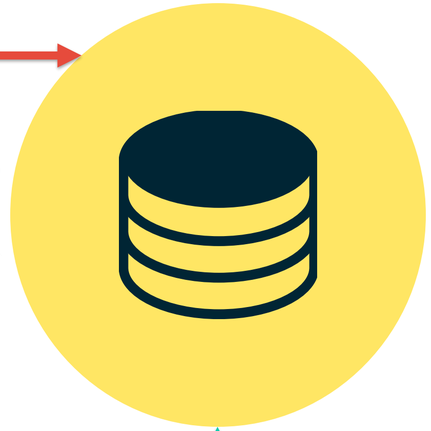
How many true positives have we seen? What's the ratio of false positives to true positives?

What's the actual dollar cost per true positive indicator we pay?


Public
Community
Low Value
High Value
Collected
Curated

Network-based Indicators

SIEM/Logs Searches & Correlation

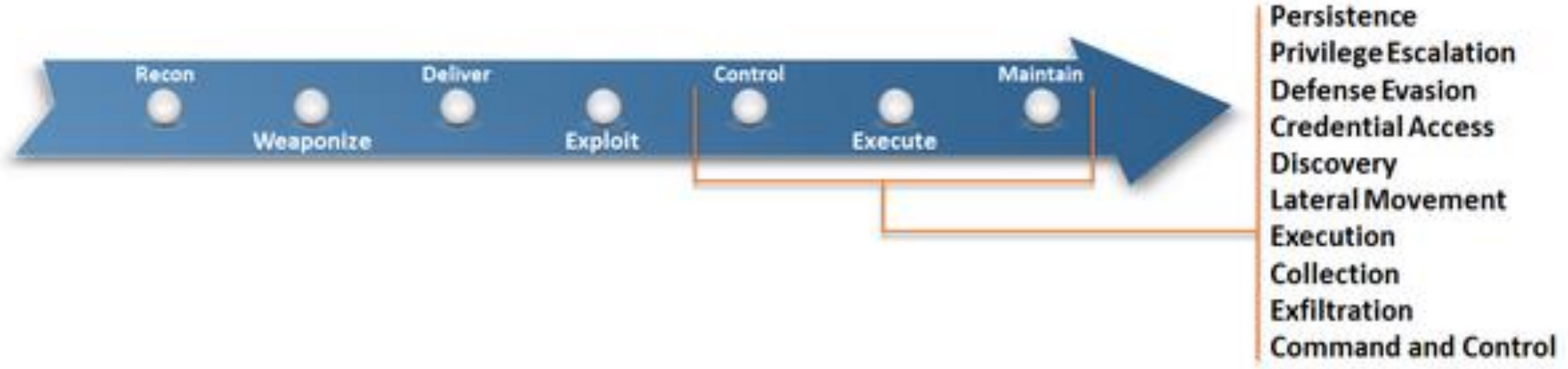


Endpoint-based Indicators

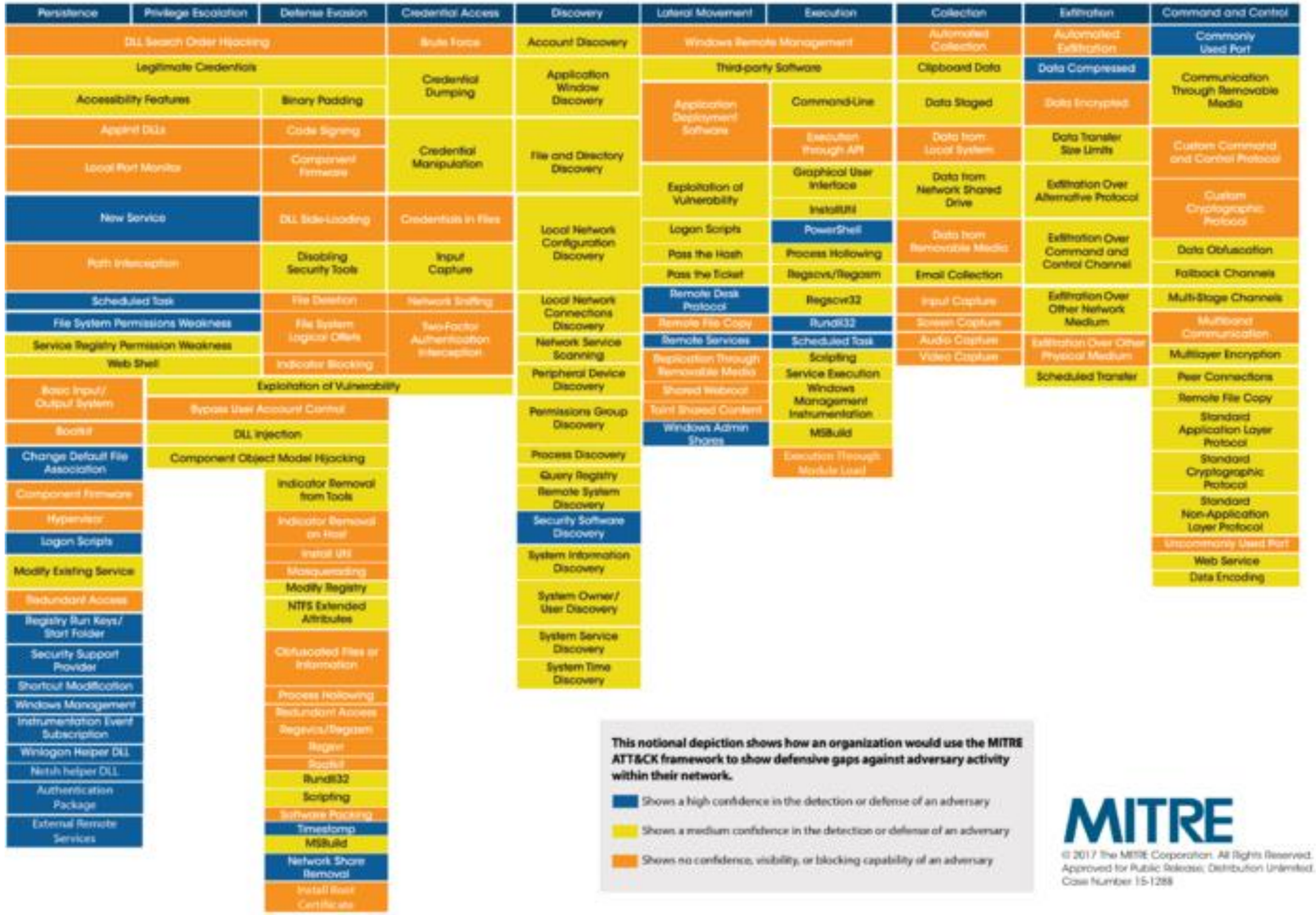
Tactics & Techniques

MITRE ATT&CK™

Adversarial Tactics, Techniques & Common Knowledge



https://attack.mitre.org



1. Develop matrix of techniques for platforms and applications in environment
2. Rate current detection capabilities for each
3. Acquire and deploy intelligence for each technique

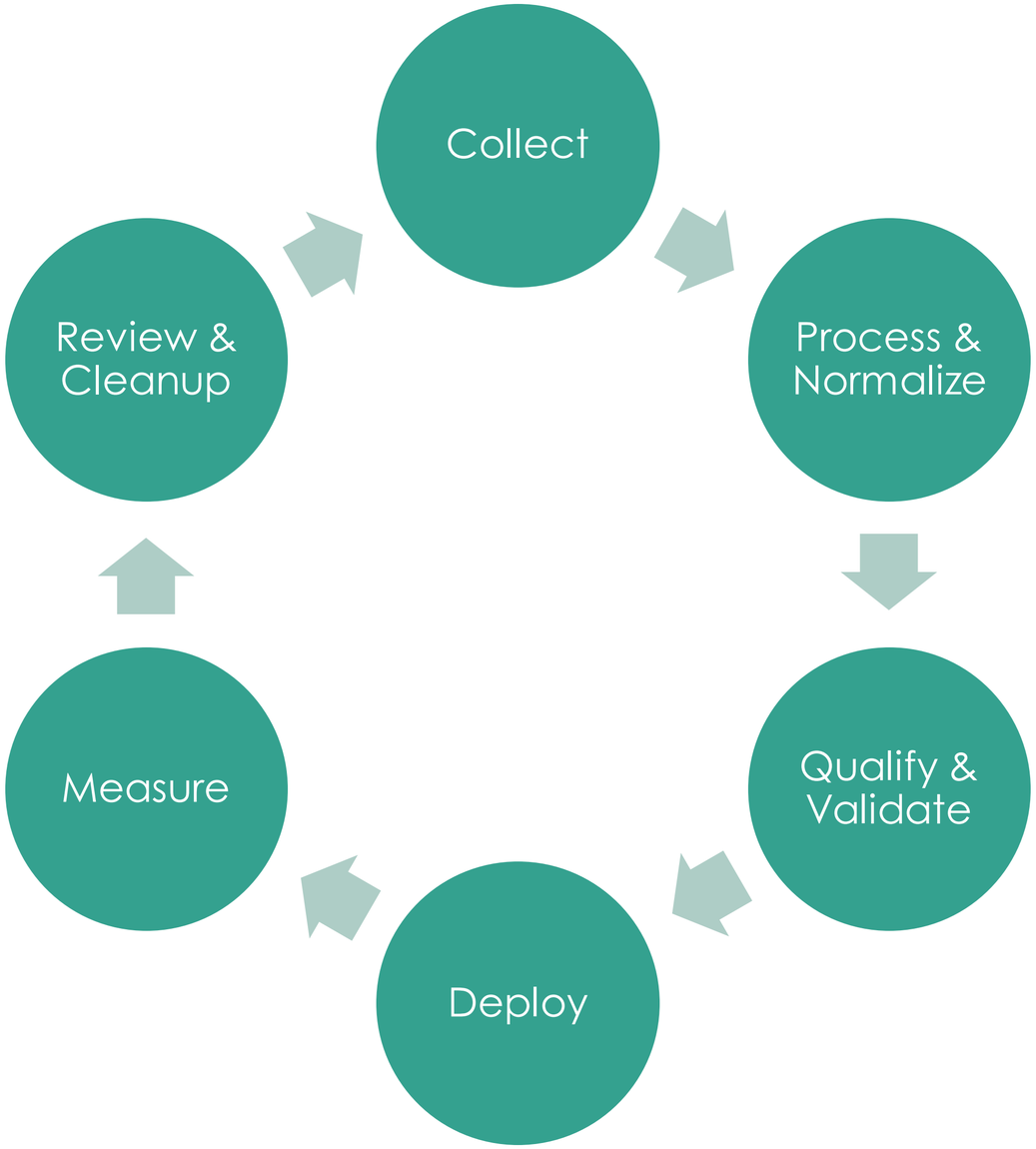
Threat Intel Challenges are process problems.

Too Much!

False Positives!

Where is it?

Stale Indicators!



Threat Intel Operational Cycle

Collect intelligence from various sources

Process intelligence and normalize into standard, machine-readable formats

Qualify and validate all indicators according to predetermined standards

Deploy to detection grid and document

Measure effectiveness and document findings for further analysis

Review results of analysis, clean up indicators that do not meet use criteria

Intelligence Management Policy

Formally document requirements for sources, indicators, detection grid, and tracking.

Outline process goals, steps, roles and responsibilities. Define metrics that quantify success and failure of each step and each resource.

Seek to collect intelligence that satisfies behavioral detection goals.

Thank You

Questions?

justin.hall@cbts.net

cbts | On a cbts company