STOP CHASING INDICATORS

A DISCUSSION ON PROACTIVE HUNT AND HOW IT CAN BE USED TO ADVANCE THREAT INTELLIGENCE

JOSH DAY / BRAD RHODES
ACCENTURE FEDERAL SERVICES

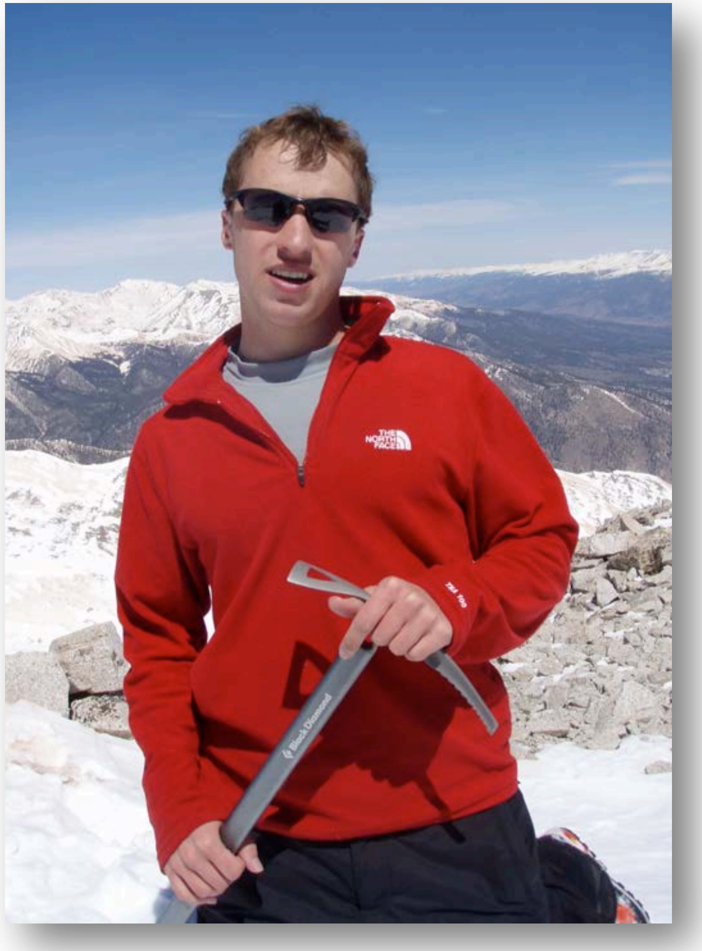
AGENDA

- INTROS
- HISTORY OF CYBER THREAT INTELLIGENCE (CTI)
- HISTORY OF THREAT HUNTING
- OUR DEFINITION OF THREAT HUNTING
- FUTURE OF CTI
- HYPOTHESIS DEVELOPMENT
- OPERATIONALIZING CTI
- THREAT HUNTING METHODOLOGIES
- NEXT-GEN CTI SHARING
- QUESTIONS

INTRODUCTIONS

JOSH DAY

- Experience:
  - 5 years @ USAF – Computer Network Operations
  - 1 year @ Endgame – Threat Hunting
  - **Currently: Accenture Federal Services – Threat Hunter**
- Areas of interest:
  - Python
  - PowerShell
  - automation (because I'm lazy)
  - code reuse (see above)
  - climbing mountains



@josh__day

INTRODUCTIONS
CONTINUED

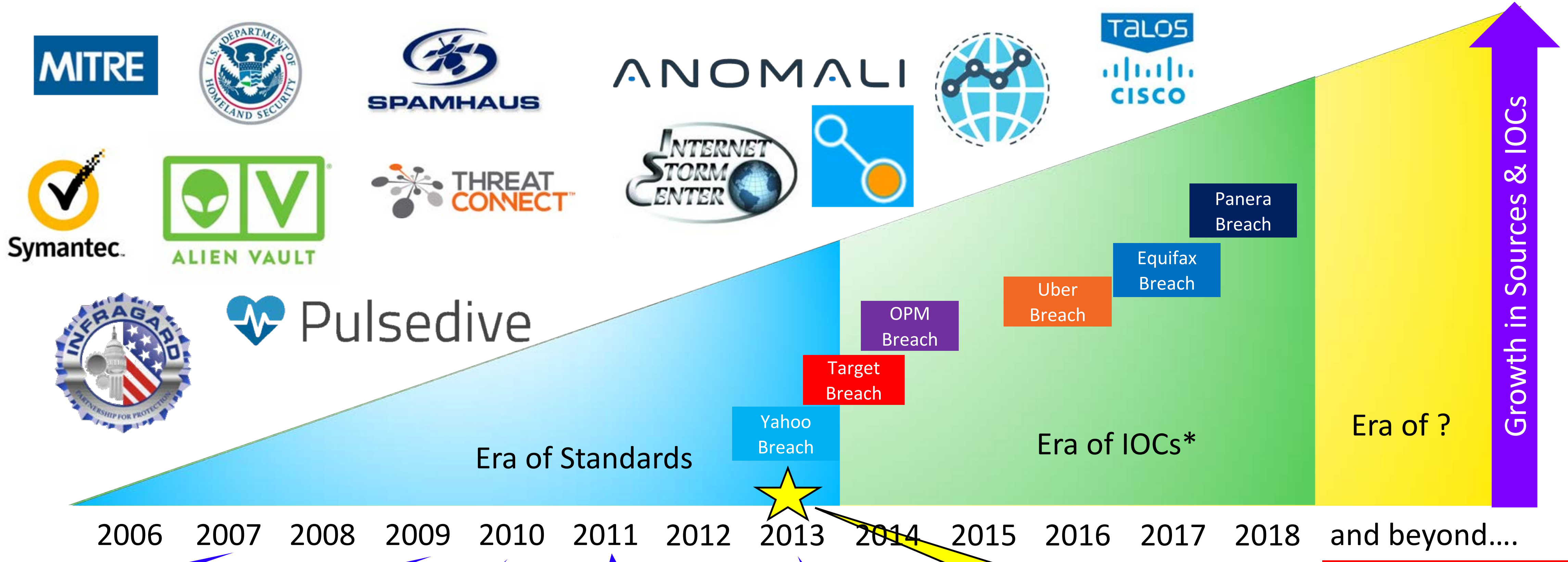
BRAD RHODES

- Experience:
  - 21+ years @ US Army & Army National Guard, Cyber Warfare
  - 18+ years DoD contractor and IC civilian
  - **Currently: Accenture Federal Services – Threat Hunter**
- Areas of Interest:
  - Elastic
  - Python
  - Big Data Analytics & Visualizations
  - Network and Packet Analysis
  - Coaching & Training

@cyber514

HISTORY OF CYBER THREAT INTEL

HISTORY OF CYBER THREAT INTELLIGENCE (CTI)



Era of Standards

Yahoo Breach

Target Breach

OPM Breach

Uber Breach

Equifax Breach

Panera Breach

Era of IOCs*

Era of ?

Growth in Sources & IOCs

2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 and beyond….

MILE-WG: IODEF

REN-ISAC: CIF

Verizon: VERIS

Mandiant: OpenIOC

AlienVault: OTX

Mitre: CyBOX, STIX, TAXII

Gartner: Threat Intelligence first defined

* Today the community gathers IOCs (raw Data) to produce Information (e.g. IDS signatures) to increase security, but that is not “intelligence”…

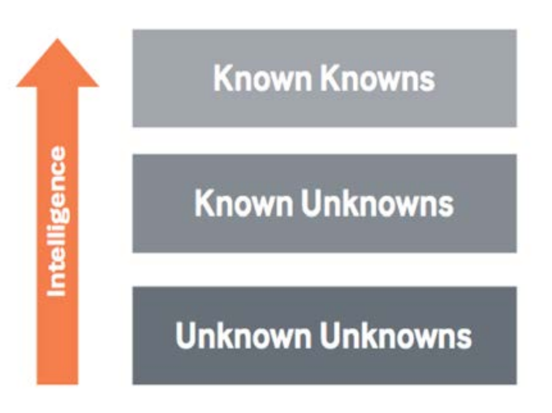
Logos are: Copyright, Trademark, Reserved by their owning organizations

HISTORY OF CTI: CTI DEFINED

From Dragos: Threat Intelligence is actionable knowledge and insight on adversaries and their malicious activities enabling defenders and their organizations to reduce harm through better security decision-making. *For intelligence quality, it must be Complete, Accurate, Relevant, and Timely.*

From Gartner: Threat Intelligence is 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. *Organizations must consider both Internal and External sources.*

From UK CERT: Threat Intelligence is information that can aid decisions, with the aim of preventing an attack or decreasing the time taken to discover an attack.



Carl von Clausewitz (On War, 1832)*:* By 'intelligence' we mean every sort of information about the enemy and his country—the basis, in short, of our own plans and operations.

From JP 2-0: The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.

Key Themes: actionable information to reduce attack impact, discover adversary activities, provide context, and support & inform decisions

HISTORY OF CTI
WHY WHAT WE'RE DOING ISN'T WORKING

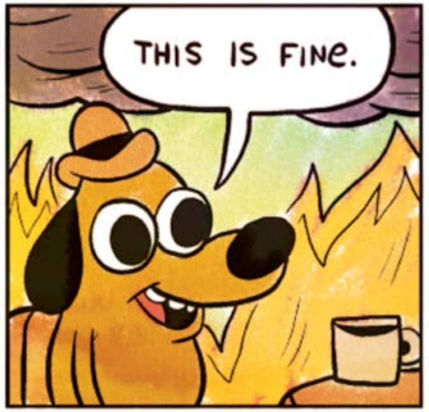
THREAT INTEL TODAY MOSTLY MEANS RAW DATA

- Multiple sources and feeds with some format standardization
- Lots and lots of raw data
- Raw data is usually refined into Information (Indicators of Compromise (IOC))

WHAT ISN'T WORKING

- Organizations consume IOCs regardless of need
- Organizations start with external sources before internal sources
- Organizations have not prioritized their assets
- Organizations are not resourced to store "mass quantities"
- Organizations cannot easily correlate events across multiple events and sources

Source: http://gunshowcomic.com/648



Source: Dreamstime.com, LLC

HISTORY OF THREAT HUNTING

HISTORY OF THREAT HUNTING

BEGINNING

- 2009 – Tony Sager (NSA/VAO) mentions hunt in context of defensive operations

- Spring 2011 – Richard Bejtlich claims to have first used the term in an article for Information Security Magazine

  To best counter targeted attacks, one must conduct counter-threat operations (CTOps). In other words, ***defenders must actively hunt intruders in their enterprise****.*

- Air Force and other DoD components have been hunting for adversaries in different networks and in different capacities for much longer than that – possibly since as early as 1998

HISTORY OF THREAT HUNTING
CONTINUED

COMMON MISCONCEPTIONS

- Hunting is searching for previously discovered indicators of compromise
  - In your enterprise
  - In your enterprise's historical data
- Hunting is investigation of alerts from SIEM or other security tool
- Hunting primarily involves running pre-fabricated scripts to find malicious behavior
  - Corollary includes black box appliance to apply AI to "hunt" for adversaries
- Hunting is just a new buzzword; we've always been "hunting"
- Hunting can be fully automated
  - Equally wrong: Hunting has to be done by humans

Source: Endgame

OUR DEFINITION OF THREAT HUNTING

OUR DEFINITION OF THREAT HUNTING

DEFINITION OF HUNT

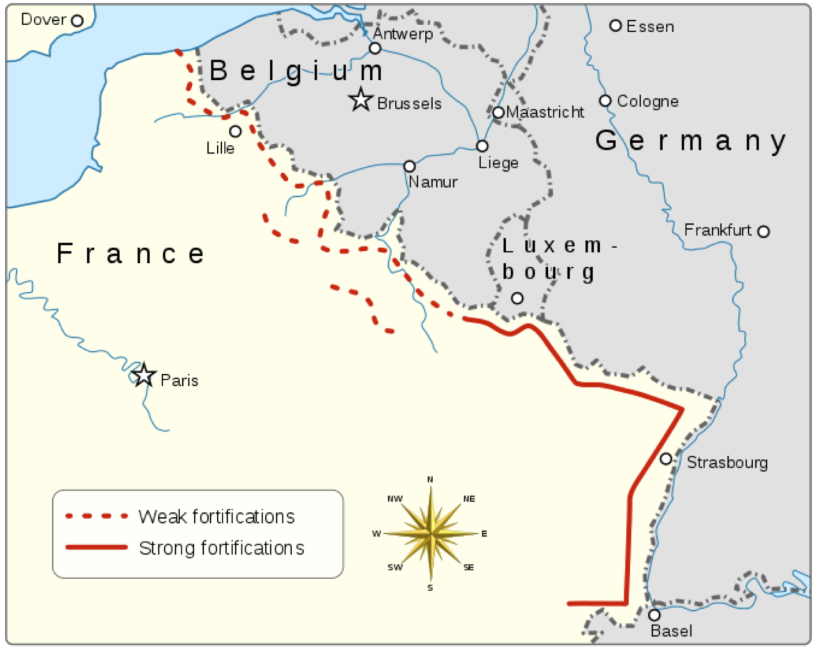
> *TO PROACTIVELY, METHODICALLY SEARCH FOR ATTACKER TECHNIQUES WITHOUT ANY INDICATION OF MALICIOUS ACTIVITY*

DON'T WAIT FOR AN ALERT TO START HUNTING…

- Focus on tactics and methods – not specific tools – to find advanced threats
- Have an offensive mindset
- Take an analytic approach

OUR DEFINITION OF THREAT HUNTING
CONTINUED

HUNT ASSUMPTIONS



https://en.wikipedia.org/wiki/Maginot_line

HACKERS ALREADY BYPASSED YOUR SECURITY MEASURES

DON'T RELY ON A MAGINOT LINE TO DEFEND AGAINST KNOWN ATTACK VECTORS

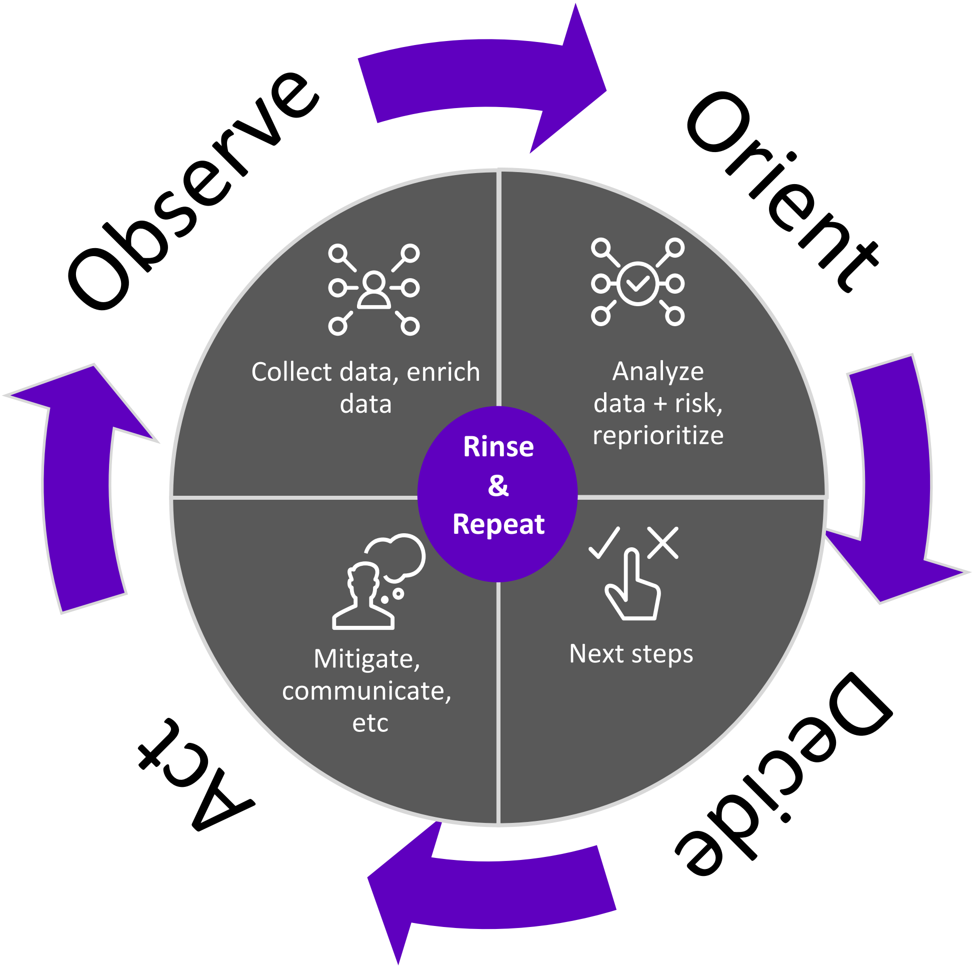
HARDENS THE PERIMETER BUT LEAVES THE DATA SOFT and CHEWY

ATTACKERS CHANGE SIGNATURES

NO SILVER BULLETS

- No software or automation will solve all your problems
- Knowledgeable **humans are always needed** to adapt to changing threat landscape

OUR DEFINITION OF THREAT HUNTING
OODA LOOP


Observe
Orient
Decide
Act
Collect data, enrich data
Analyze data + risk, reprioritize
Next steps
Mitigate, communicate, etc
Rinse & Repeat

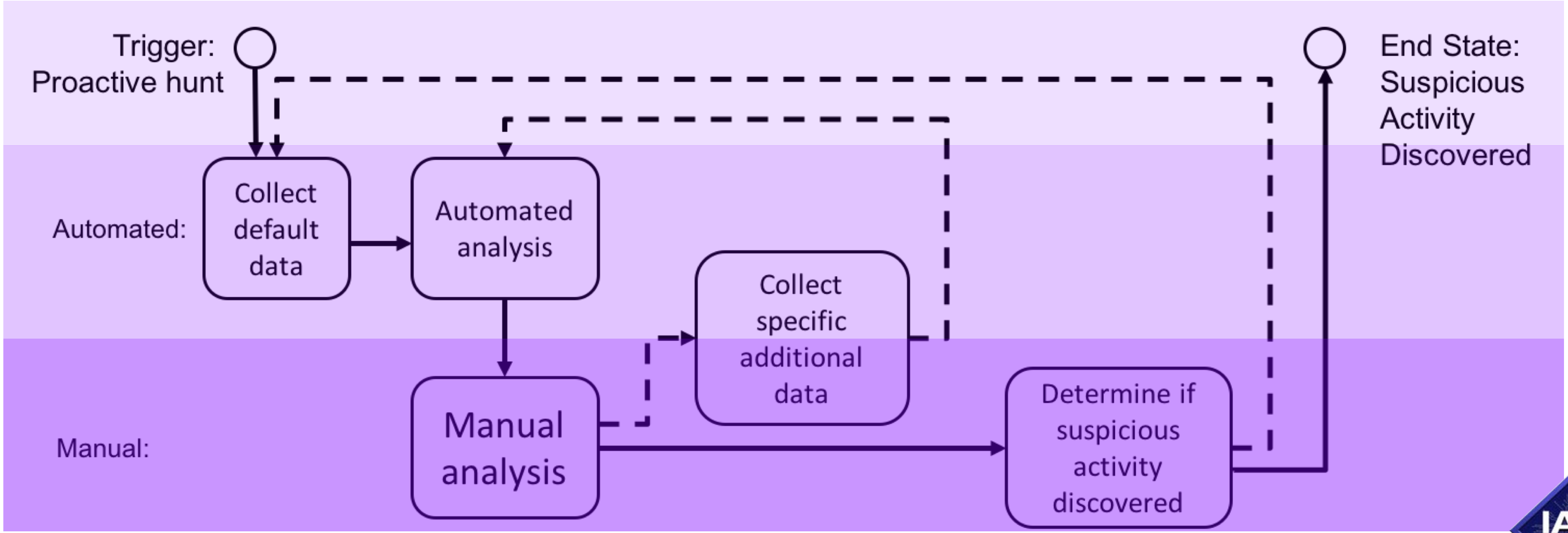
Always increasing speed

To outpace adversary

OUR DEFINITION OF THREAT HUNTING
SAMPLE WORKFLOWS

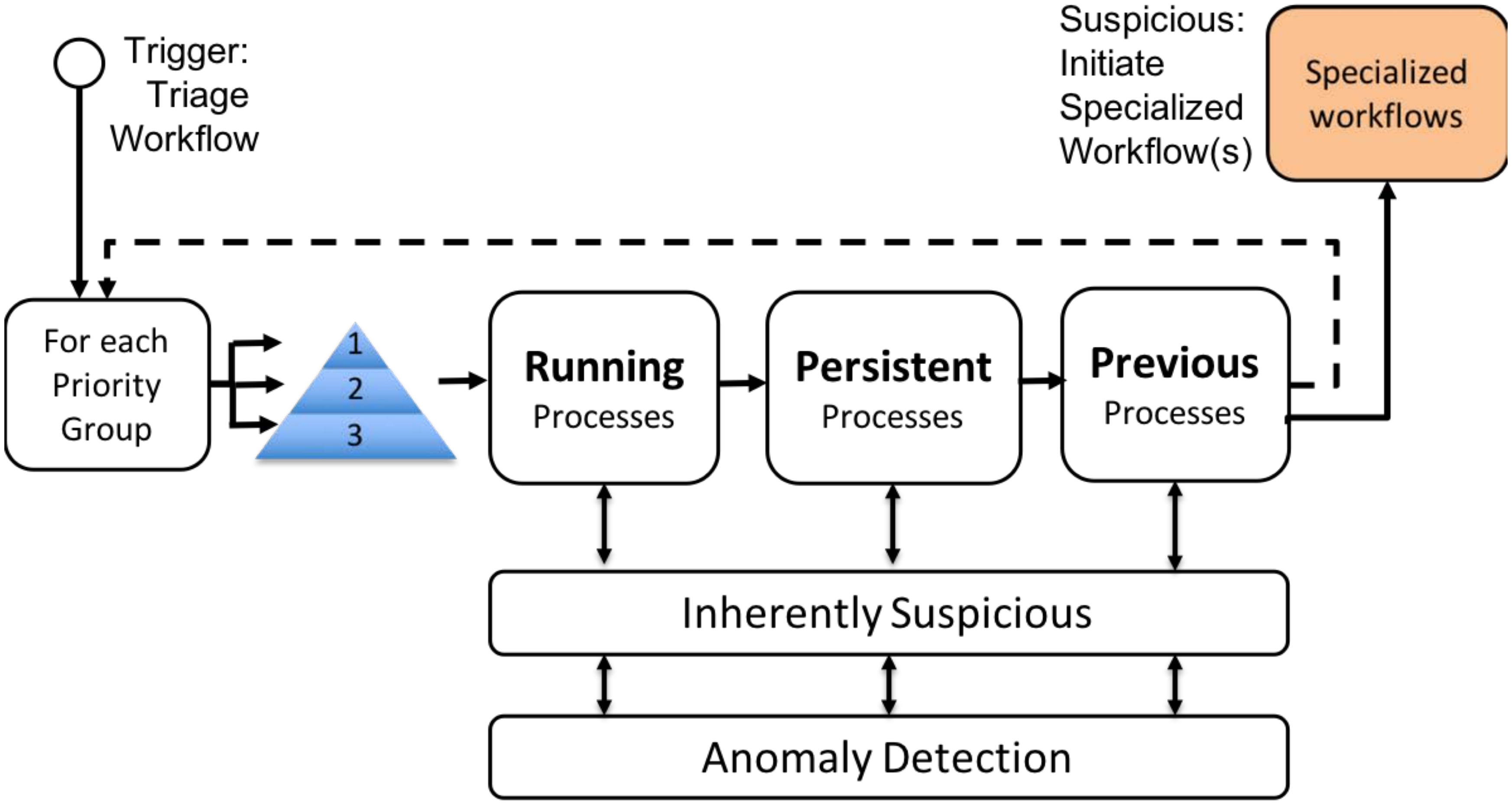
Proactive Hunting Methodology

adapted from OODA loop



https://www.iacdautomate.org/

OUR DEFINITION OF THREAT HUNTING
SAMPLE WORKFLOWS (CONT.)



FUTURE OF CTI

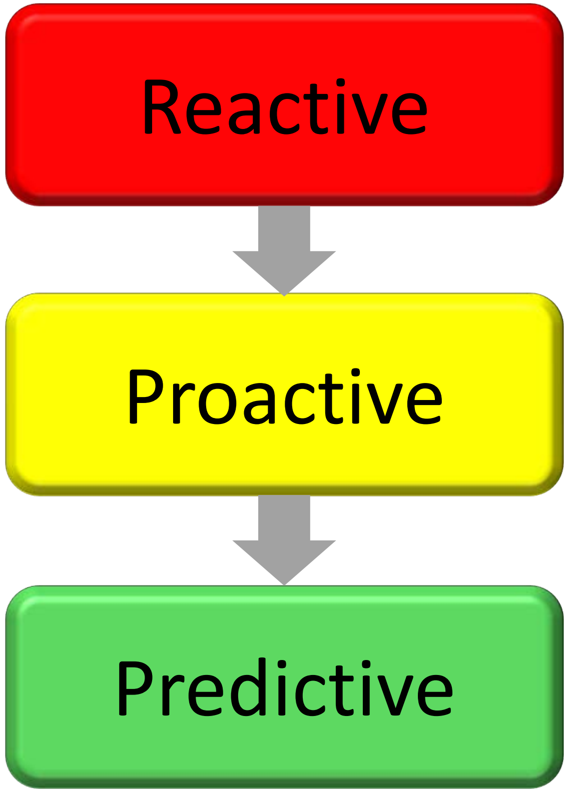
FUTURE OF CTI
NEXT-GEN

PLEASE DON'T STONE US

- Traditional indicator sharing and distribution isn't going away (and shouldn't)
- Just because you can ingest a horde of IOCs doesn't mean you should
- The jury is out on the veracity of some CTI sources
- No matter how many analysts & tools you have, it will never be enough

INTELLIGENCE DRIVEN ORGANIZATIONS…

- Have leadership buy-in
- Are selective on sources
- Are process oriented
- Have priorities
- Are integration focused

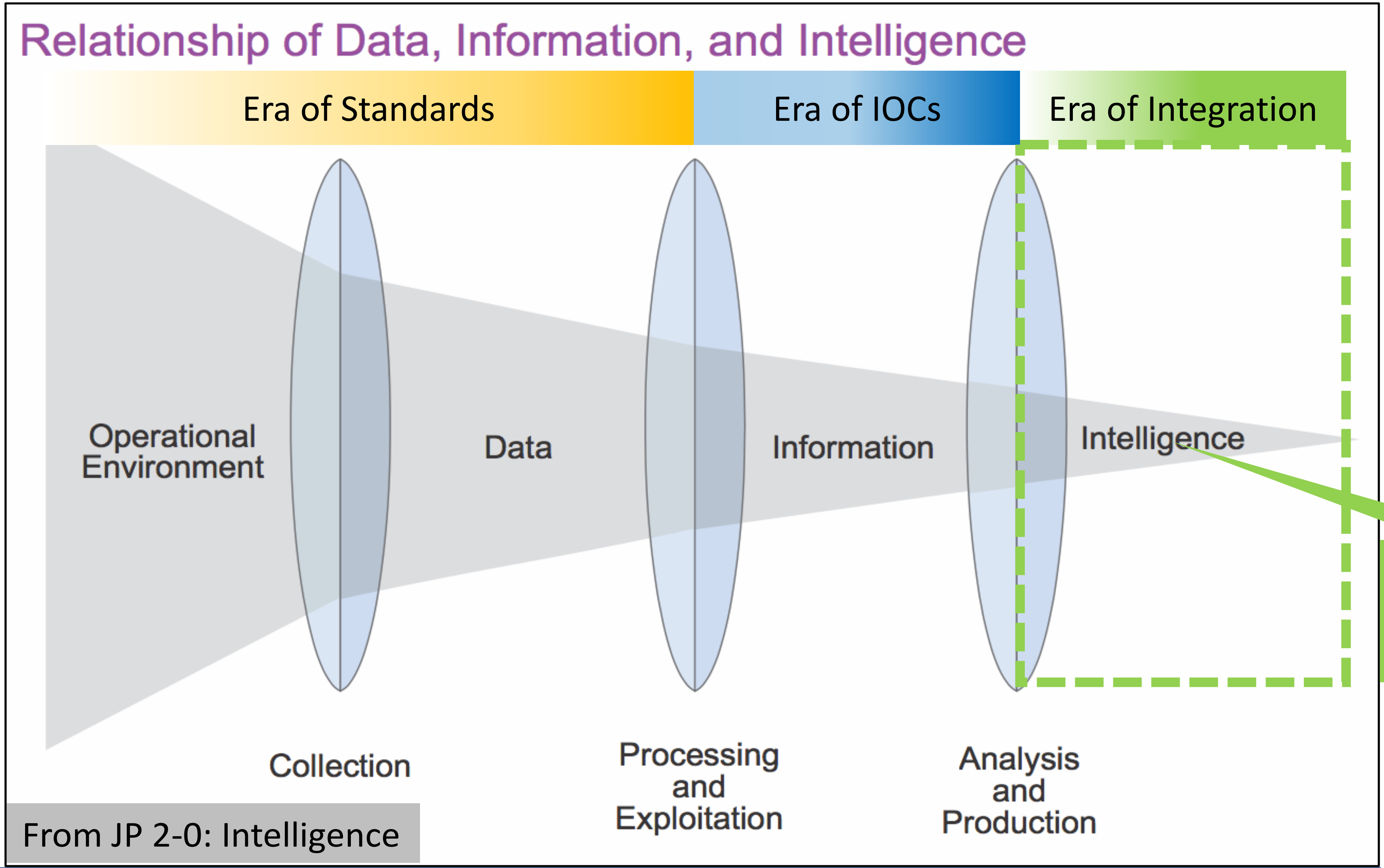


Reactive

Proactive

Predictive

ERA OF INTEGRATION

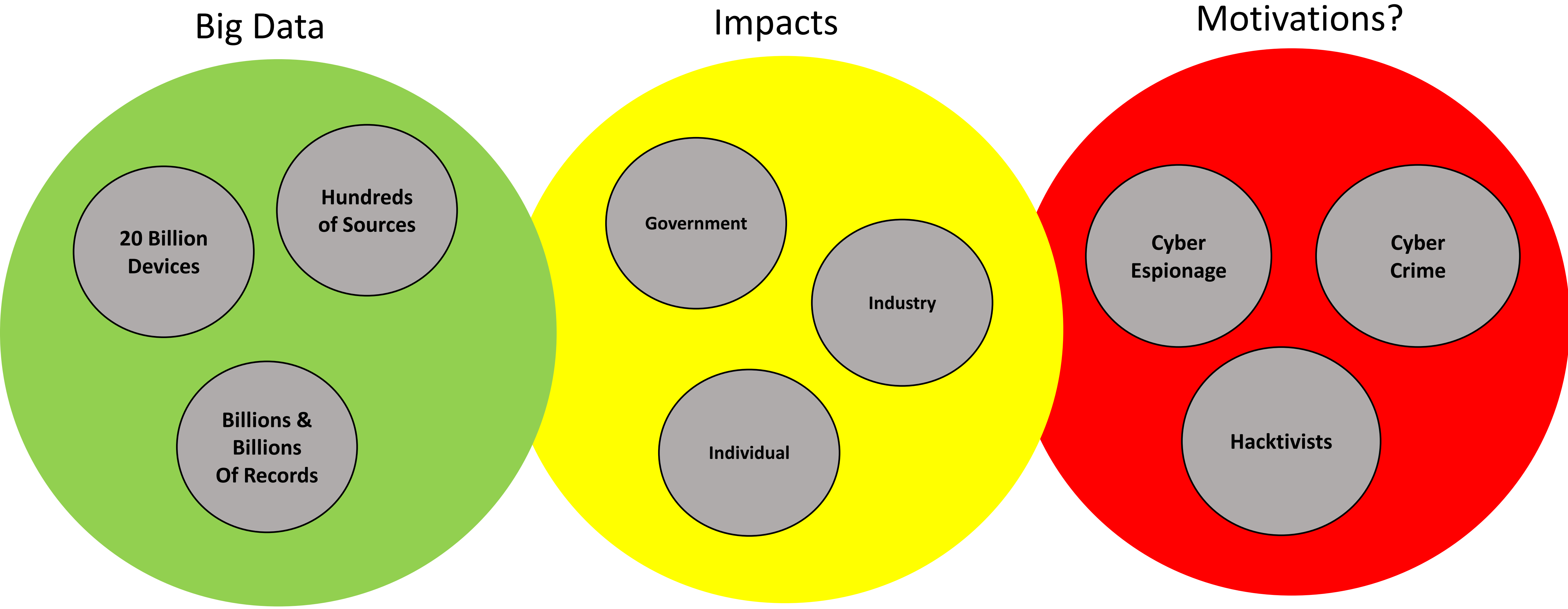


From JP 2-0: Intelligence

Focused Products are the new CTI value proposition!

Today, we harvest IOCs (raw Data) to produce Information (to improve security), NOW we need to create Intelligence (products to support risk-based decisions)!

OPERATIONALIZING CTI – BIG ROCKS



Big Data

20 Billion Devices

Hundreds of Sources

Billions & Billions Of Records

Impacts

Government

Industry

Individual

Motivations?

Cyber Espionage

Cyber Crime

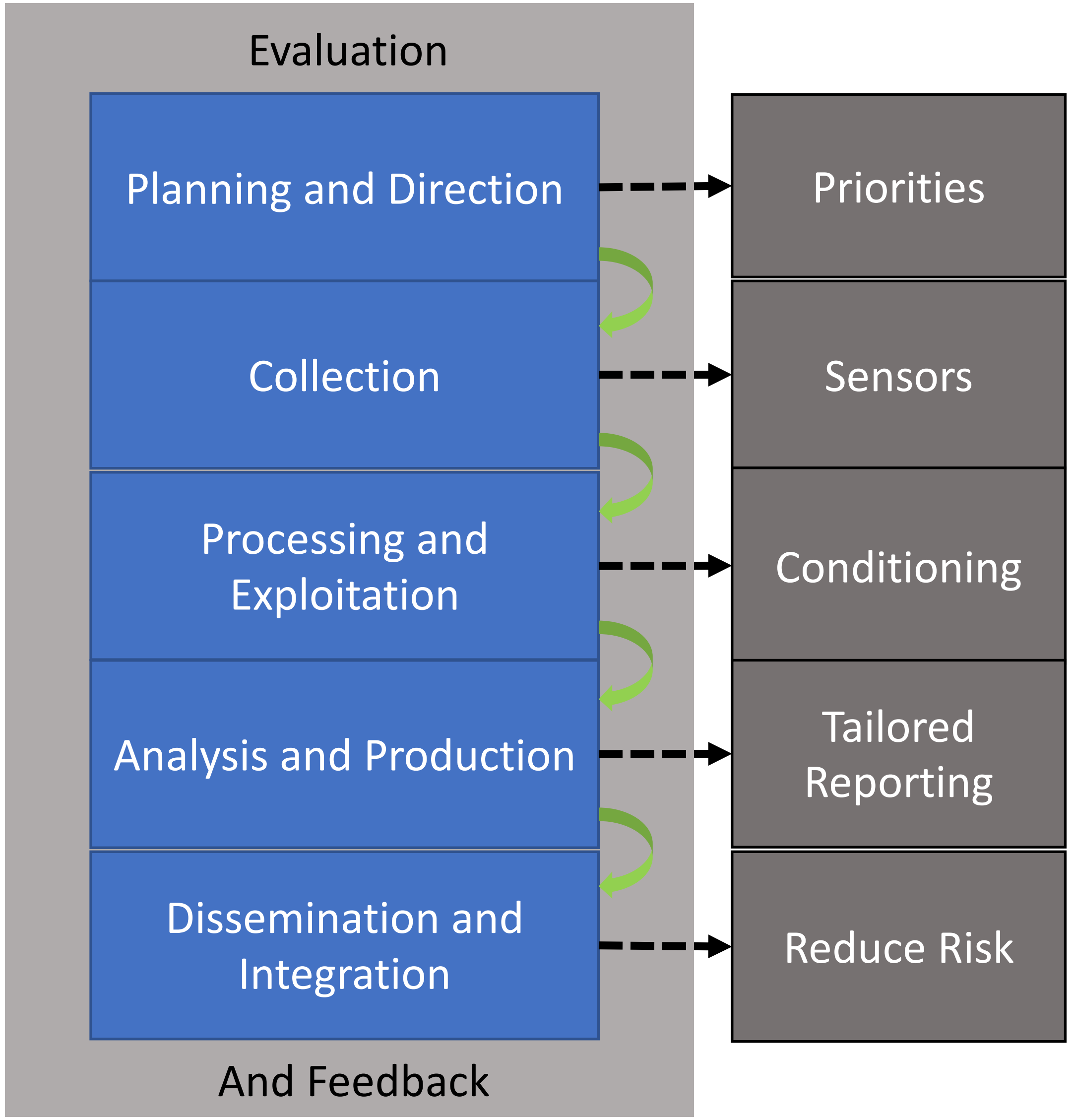
Hacktivists

Stop throwing more data at the problem!!

Every organization has different intelligence requirements

Context is for Kings (why are certain TTPs used against an organization)?

OPERATIONALIZING CTI – HOW?



Evaluation

Planning and Direction

Collection

Processing and Exploitation

Analysis and Production

Dissemination and Integration

And Feedback

Priorities

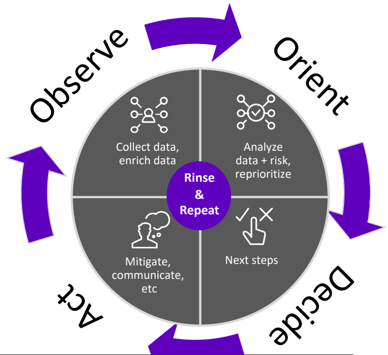
Sensors

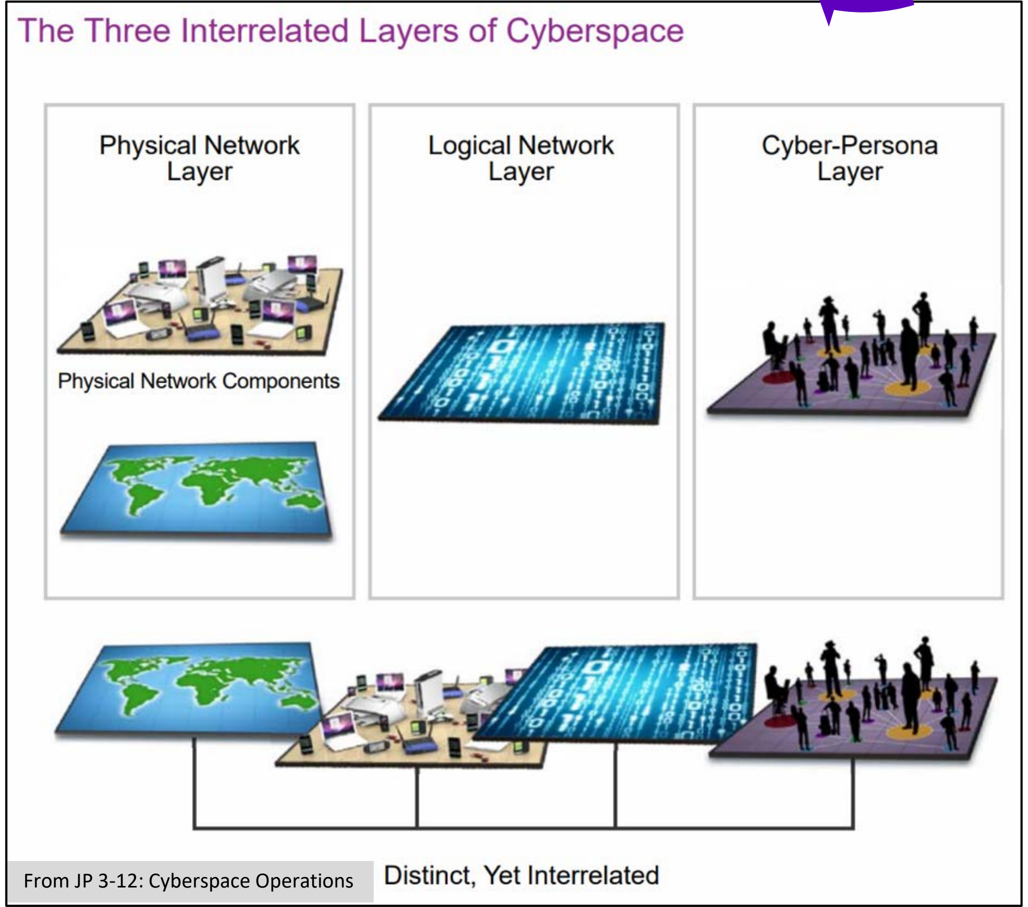
Conditioning

Tailored Reporting

Reduce Risk

Why?


Observe
Orient
Decide
Act
Collect data, enrich data
Analyze data + risk, reprioritize
Rinse & Repeat
Mitigate, communicate, etc
Next steps

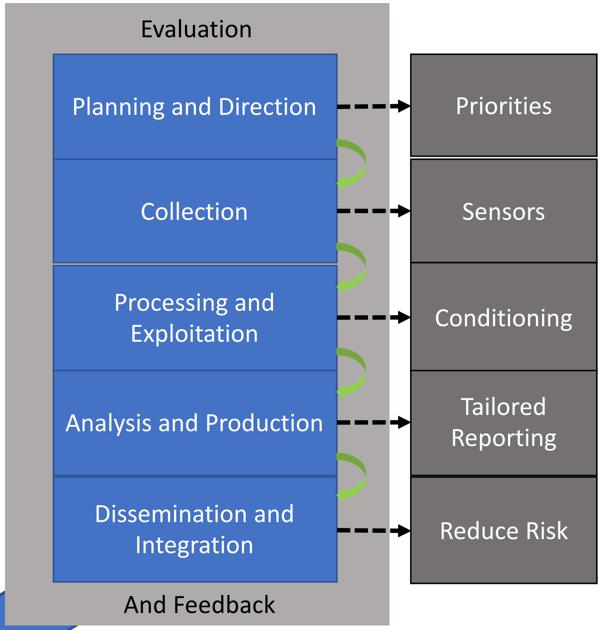

The Three Interrelated Layers of Cyberspace

From JP 3-12: Cyberspace Operations

OPERATIONALIZING CTI - EXAMPLE

PRE-ATT&CK™
ATT&CK™

Source: Mitre


Evaluation

Planning and Direction → Priorities

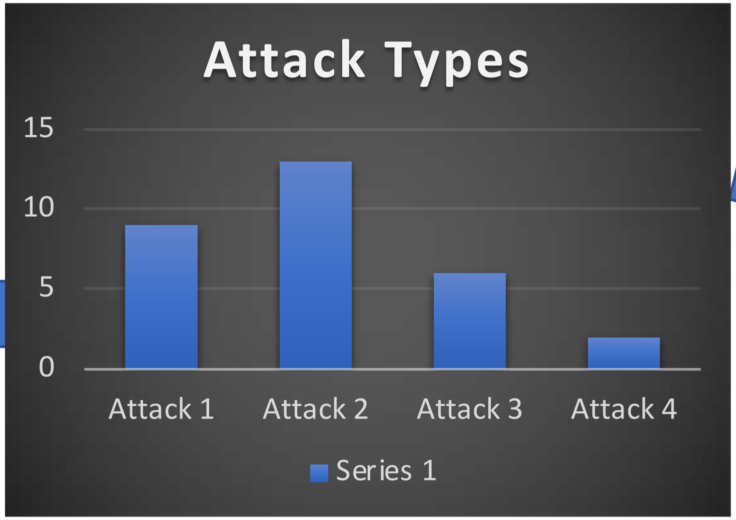
Collection → Sensors

Processing and Exploitation → Conditioning

Analysis and Production → Tailored Reporting

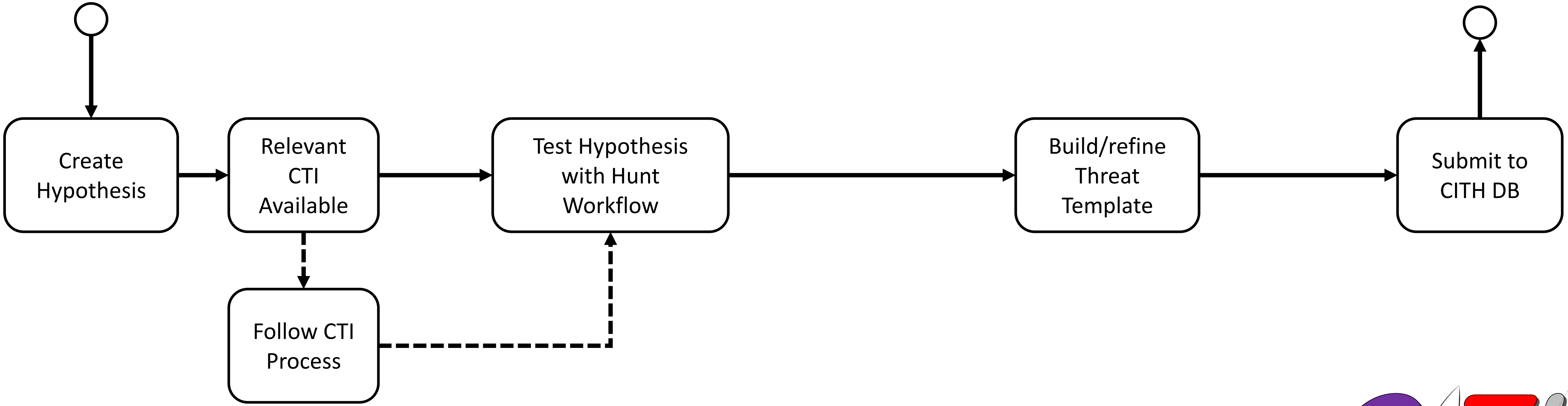
Dissemination and Integration → Reduce Risk

And Feedback



Informed Decision

NEXT-GEN CTI
PLAYBOOK



Create Hypothesis

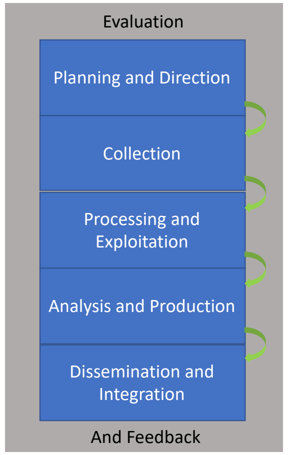
Relevant CTI Available

Test Hypothesis with Hunt Workflow

Build/refine Threat Template

Submit to CITH DB

Follow CTI Process



Evaluation

Planning and Direction

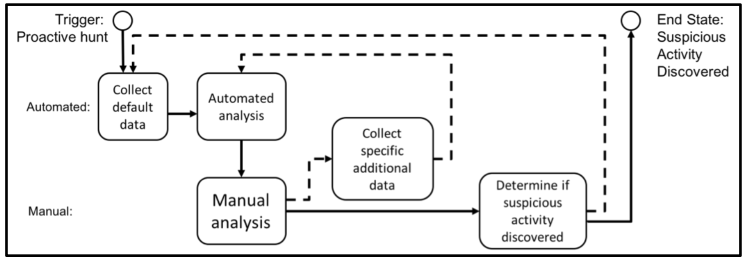
Collection

Processing and Exploitation

Analysis and Production

Dissemination and Integration

And Feedback



Trigger: Proactive hunt

Automated:

Collect default data

Automated analysis

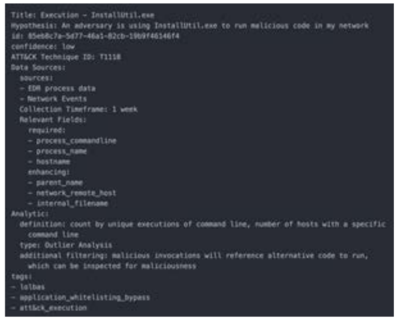
Collect specific additional data

Manual:

Manual analysis

Determine if suspicious activity discovered

End State: Suspicious Activity Discovered



```
Title: Execution - InstallUtil.exe
Hypothesis: An adversary is using InstallUtil.exe to run malicious code in my network
id: 85eb8c7a-5d77-46a1-82cb-19b9f46146f4
confidence: low
ATT&CK Technique ID: T1118
Data Sources:
  sources:
  - EDR process data
  - Network Events
  Collection Timeframe: 1 week
  Relevant Fields:
    required:
    - process_commandline
    - process_name
    - hostname
    enhancing:
    - parent_name
    - network_remote_host
    - internal_filename
Analytic:
  definition: count by unique executions of command line, number of hosts with a specific
    command line
  type: Outlier Analysis
  additional filtering: malicious invocations will reference alternative code to run,
    which can be inspected for maliciousness
tags:
- lolbas
- application_whitelisting_bypass
- att&ck_execution
```

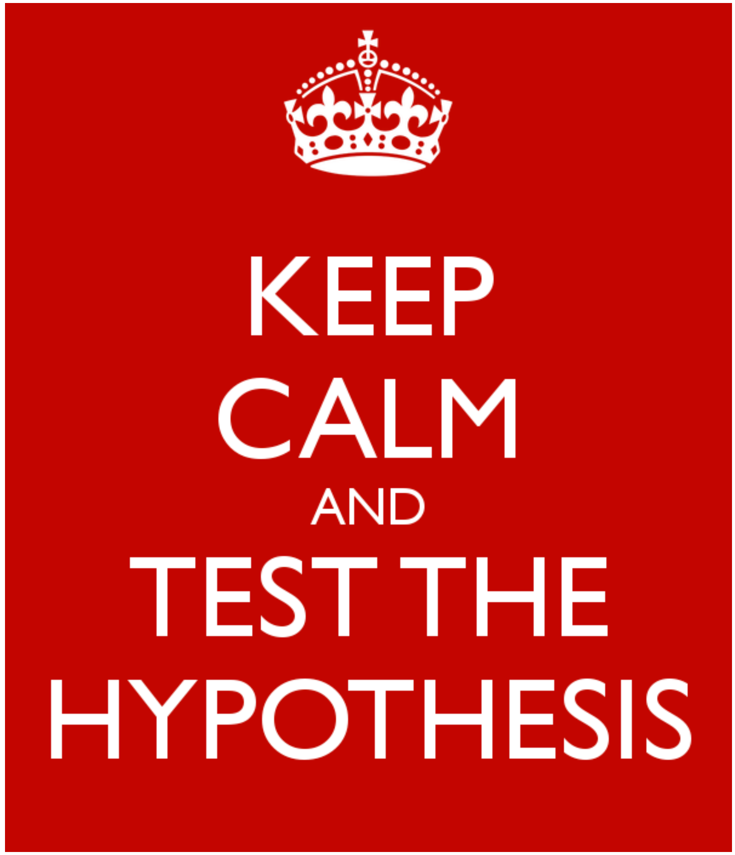
Cyber Intelligence & Threat Hunt (CITH*) Database

*Pronounced “Sith”

NEXT-GEN CTI
PLAYBOOK DETAILS

HYPOTHESIS CREATION

- Decide on a question to ask
  - Could be from analyst experience, recent reporting, or other sources
- A good hypothesis is testable – otherwise it's just an assumption
  - Generally, we want our hypotheses to be technique or procedure specific
- If you aren't asking the right questions, then you are wasting your time – **so ask good questions**
- To start, ask questions where you have data collection to answer those questions
  - Next step would be to ask questions that require more data collection



Source: http://workingwithmckinsey.blogspot.com/2014/02/Being-Hypothesis-Driven.html

NEXT-GEN CTI
PLAYBOOK DETAILS (CONT.)

CTI PROCESS

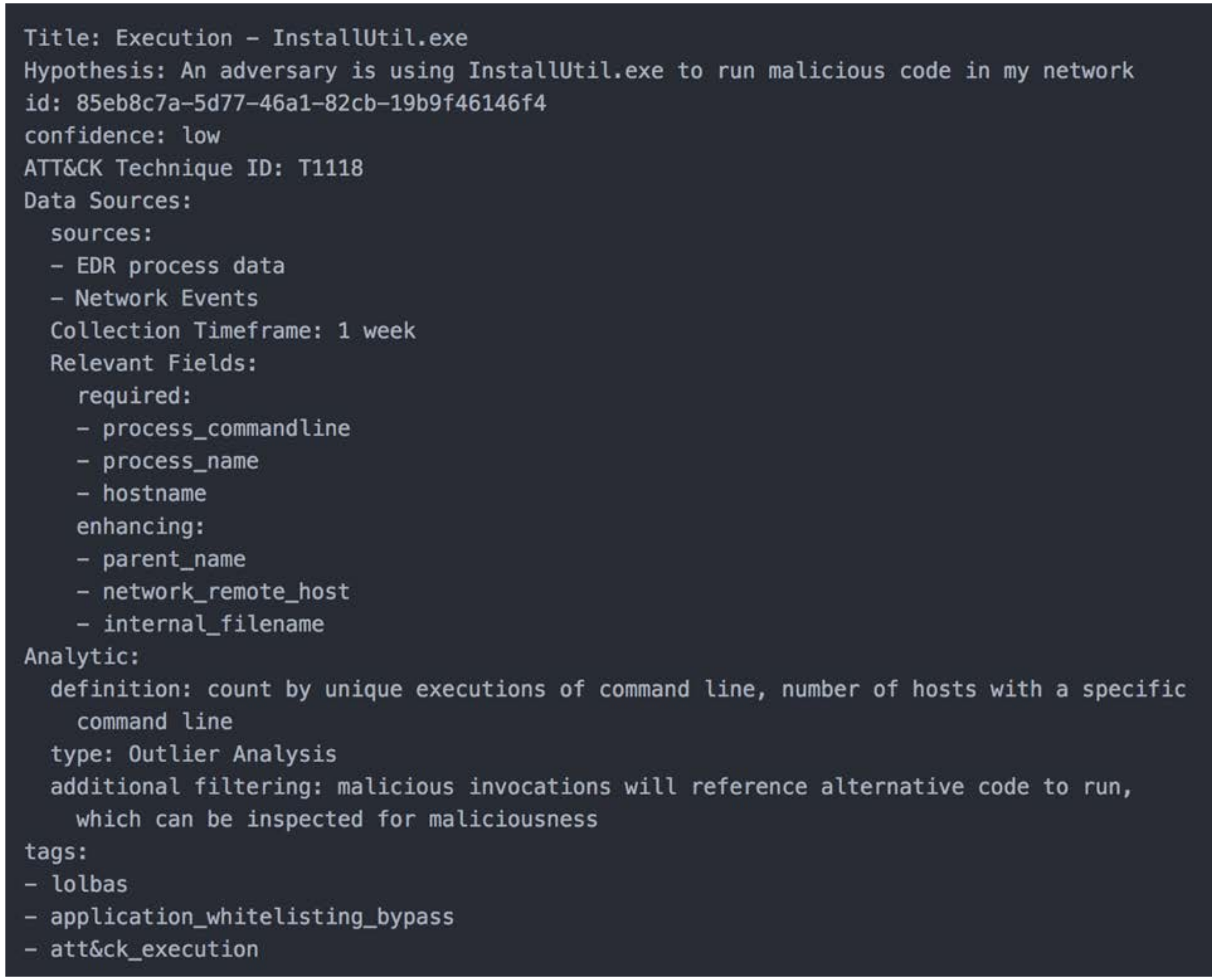
- First, check the CITH DB and existing organization sources for CTI related to the hypothesis
- If none, develop environment focused **Requirements** (Planning & Direction), **Collect** (raw data via sensors), **Process and Exploit** (information), **Analyze and Produce** (CTI products), and finally **Integrate** (CTI) into the hunt workflow
- If the end result of the hunt workflow is discovery of threat actions in the environment, the are hypothesis and CTI validated leading to creation of a Threat Template for ingest in the CITH DB

CITH DB EXAMPLE

NEXT-GEN CTI
CITH TEMPLATE

CITH ENTRY EXAMPLE

- Title for entry and hypothesis
- Linked to MITRE ATT&CK by technique ID
- Shows data fields and data sources for identification
- Analytics listed for discovery of attacker technique and methods for additional filtering
- Confidence level and associated tags for searching
- Potential sources: https://www.threathunting.net, https://github.com/Neo23x0/sigma, MITRE ATT&CK



```
Title: Execution - InstallUtil.exe
Hypothesis: An adversary is using InstallUtil.exe to run malicious code in my network
id: 85eb8c7a-5d77-46a1-82cb-19b9f46146f4
confidence: low
ATT&CK Technique ID: T1118
Data Sources:
  sources:
  - EDR process data
  - Network Events
  Collection Timeframe: 1 week
  Relevant Fields:
    required:
    - process_commandline
    - process_name
    - hostname
    enhancing:
    - parent_name
    - network_remote_host
    - internal_filename
Analytic:
  definition: count by unique executions of command line, number of hosts with a specific
    command line
  type: Outlier Analysis
  additional filtering: malicious invocations will reference alternative code to run,
    which can be inspected for maliciousness
tags:
- lolbas
- application_whitelisting_bypass
- att&ck_execution
```

NEXT-GEN CTI
CITH TEMPLATE (CONT.)

OTHER FIELDS

- Applicable industries (if any)
  - Especially critical infrastructure
- Contributor(s)
- Dates (modification, creation)
- References
- Optional notes

NEXT-GEN CTI
CITH TEMPLATE (CONT.)

HUNT TEAM CONSUMES CITH ENTRIES

- Decide specific implementation with organization’s data
- **Keep in mind:** some high confidence analytics in one organization may be low confidence in another

HUNT TEAM EVALUATES RESULTS

- Evaluate analytic performance with specific organizational makeup
- After manual validation of analytic within organization, automation should be considered
  - Focus automation on high confidence analytics
- CITH entries should be tweaked and re-distributed when issues are discovered
  - Like Wikipedia for threat hunting intelligence

NEXT-GEN CTI
CITH TEMPLATE (CONT.)

GOOD NEWS!!

- The CITH DB concept is already on its way!

https://car.mitre.org/wiki/Main_Page

+

https://nsacyber.github.io/unfetter/index.html

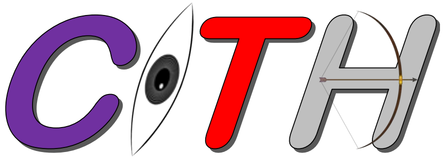
+

Context

&

Courtesy of DHS

=



Using these starting points, CITH can be quickly scaled to provide curated CTI for the community!

NEXT-GEN CTI
SHARING

NOT SHARING IS NO LONGER AN OPTION

- Leverage our ISACs and ISAOs
- Sanitization and automation
  - Human readable tearlines
  - Machine-to-machine (wider adoption of STIIX/TAXII/CYBOX)
- Get to the point where there is more open sharing!
  - Communities of like environments should be talking about their CTI requirements
- Data sharing goes both ways
- Build products that help create decision points, not just pretty pictures
- Utilize the CITH DB to improve levels of threat hunting maturity by contributing!!

Source: https://wolfgangsuetzl.net/2011/11/20/cultures-and-ethics-of-sharing/

NEXT-GEN CTI
WHAT'S NEXT

OUR ACTION

- Keep pushing this model
- Put our own in-house analytics into CITH format

COMMUNITY ACTION

- Information distribution framework
  - Allow for information to flow both ways
  - Yelp for hunt analytics
- Everyone has something to contribute
  - Unique detections
  - Industry-specific threats

QUESTIONS?