PLEASE DOWNLOAD IF YOU DID NOT RECEIVE THE LINK BEFOREHAND

http://bit.ly/2ETs3Of

CHRIME

BY MONTY ST JOHN

Monty St John

Who is this guy?

- 25 years of security and analytics – physical, investigations, information, computer forensics, reverse engineering, threat intelligence
- Two decades supporting federal, state, and local LE while in uniform

Forensics and Threat Intelligence

- Better part of past decade acting as a key member of forensic and TI teams deconstructing, analyzing and providing insights into threats and how to thwart them

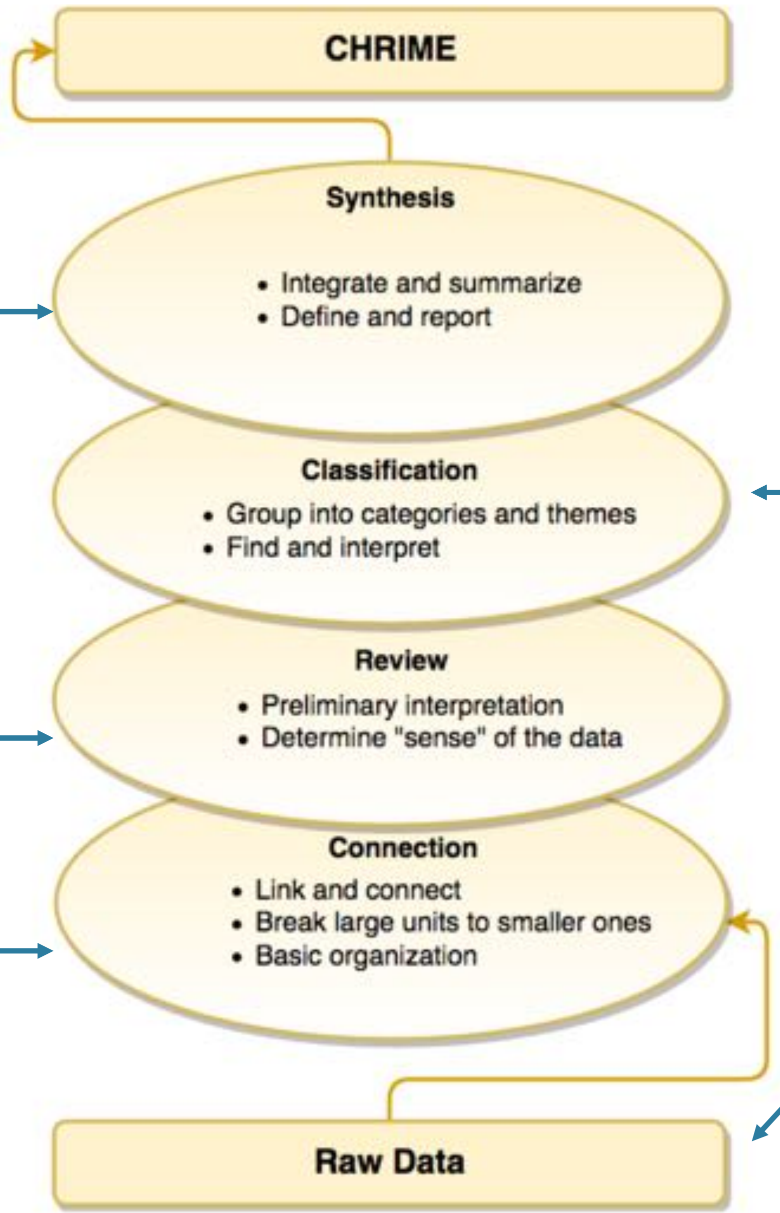
BACKGROUND

IT STARTS AT THE BEGINNING

CHRIME's Story

- Born out of frustration and a need for standardized approach to analysis driven requests (think TI/SOC).
- Needed to be fast but not so quick that accuracy was lost.
- Completeness was required, but not to the point of becoming time consuming.
- Had to approach any problem from multiple directions.

CHRIME was built to help handle issues like ransomware and to help make sure we would never have to issue or retract messages, like they did in Hawaii recently.



CHRIME

Synthesis

- Integrate and summarize
- Define and report

Classification

- Group into categories and themes
- Find and interpret

Review

- Preliminary interpretation
- Determine "sense" of the data

Connection

- Link and connect
- Break large units to smaller ones
- Basic organization

Raw Data

Where does it fit?

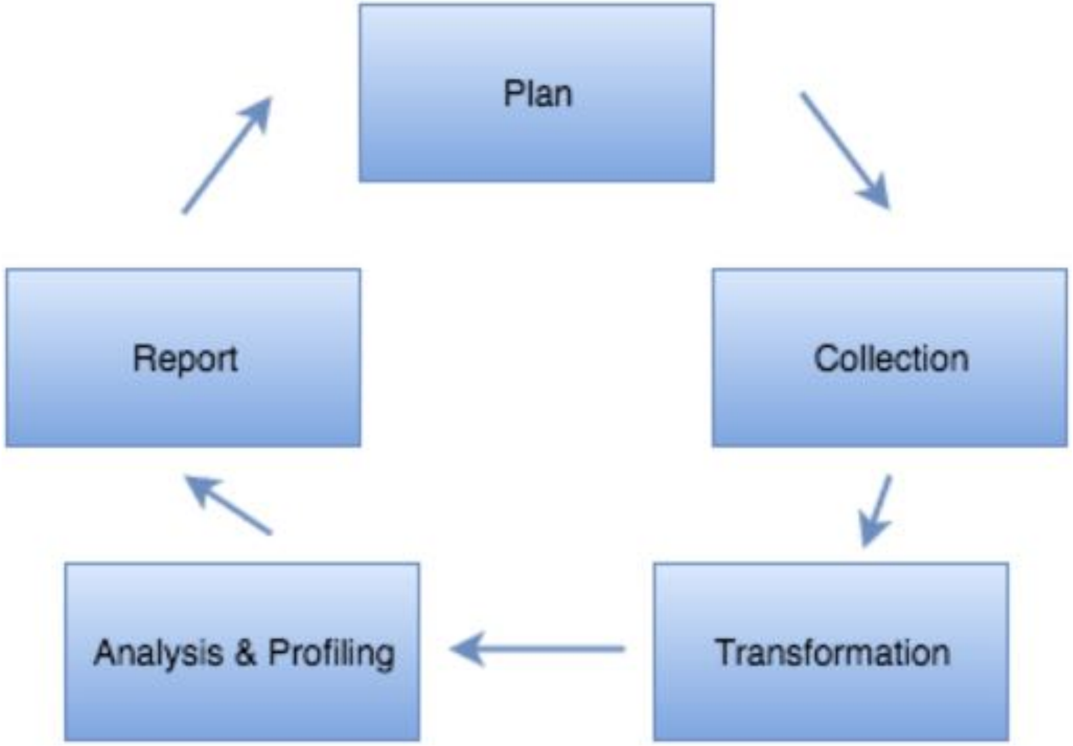
What do I do with this information?

What does this mean?

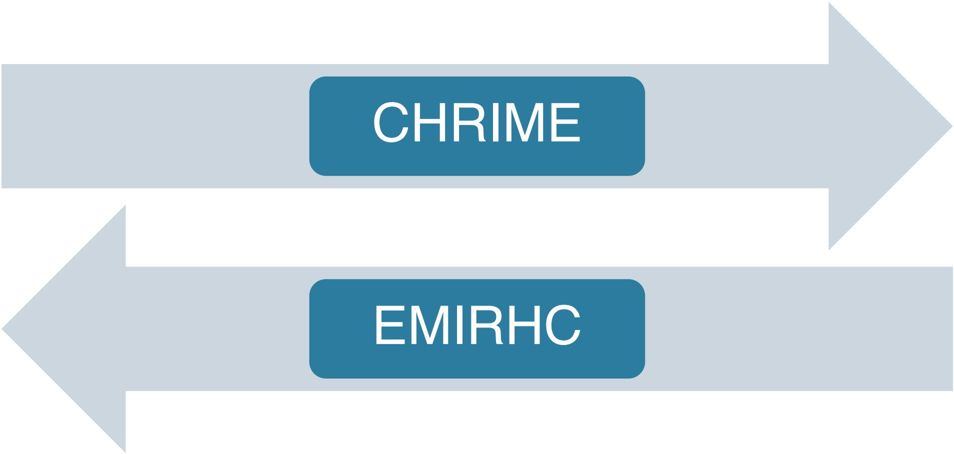
Does it link to something else I know?

What am I seeing here?

CHRIME is a streamline of the normal intelligence cycle



- CHRIME was crafted to hasten decisions
- It mnemonically identifies six data categories to handle “field issues” common to security operations and threat intelligence
- Everything in CHRIME starts with the tactical decision being made



CHRIME

EMIRHC

- CHRIME is about decisions. Tactical decisions:
  - Block? Allow?
  - Whitelist? Blacklist?
  - Monitor? Ignore?
  - Threat? Suspicious? Benign?
  - Persistent? One-off?
  - False positive? False Negative?

WHAT?
WHAT?
WHAT?

A decision to be made and then:

- Constellation - maps of data
- History
- Reputation
- Intent
- Malware - or, modus operandi
- Execution - actions and operations evaluated, either by inference, observation or both

CHRIME is both Hard and Soft

- Why these six topics?
- Why in that particular order?
- Beyond a handy acronym, three of them represent the “hard” variables of ‘C’, ‘M’, and ‘E’
- The internal ‘H’, ‘R’, and ‘I’ represent the “soft” variables

COMPONENTS

BREAKING IT DOWN

Before CHRIME starts…

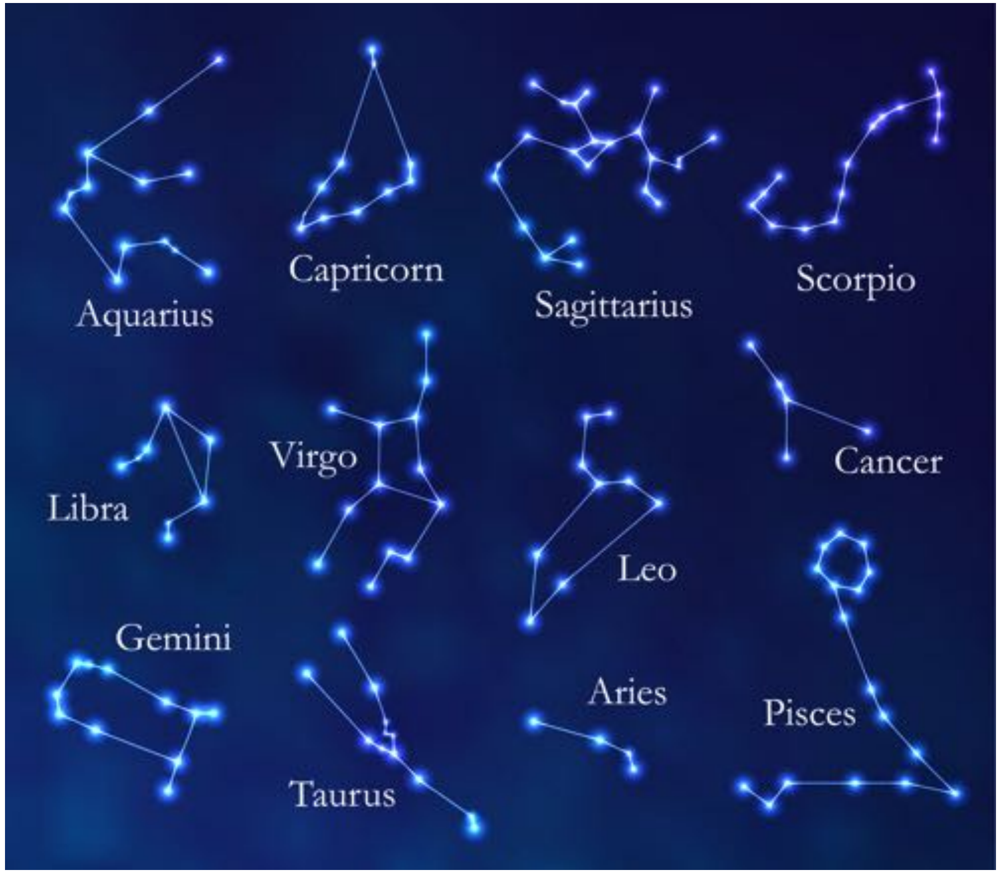
One question to rule them all

- CHRIME begins by boiling down the problem to a single question and, if possible, with a single answer.
- Complex questions should be broken down before beginning, e.g., use Framing techniques.

Framing exercise

- **Constellations** are exactly what they sound like, though instead of a star map to guide travelers it represents a group of linked elements that serve the same purpose.

- Just like aligning to a constellation in the sky can tell you many things, so can constellations of files, dns, identities, relationships, etc.



Just like in the past when constellations were used for agriculture, to know when to plant and harvest, you can **employ this kind of mapping to identify when a threat actor, a tactic or technique** is being employed (i.e., by the structure of things).

- Constellations can pivot around any single point in their structure and go as deep as needed to connect data

- Allows for determination of **what is present** versus **what should be present**

- Key is to capture immediate links and then deeper as needed or required

- Our experience shows that ~44% of tickets were answerable purely from drafting a map

What I should See

What I do see

Constellation exercise

www.cyberdefenses.com

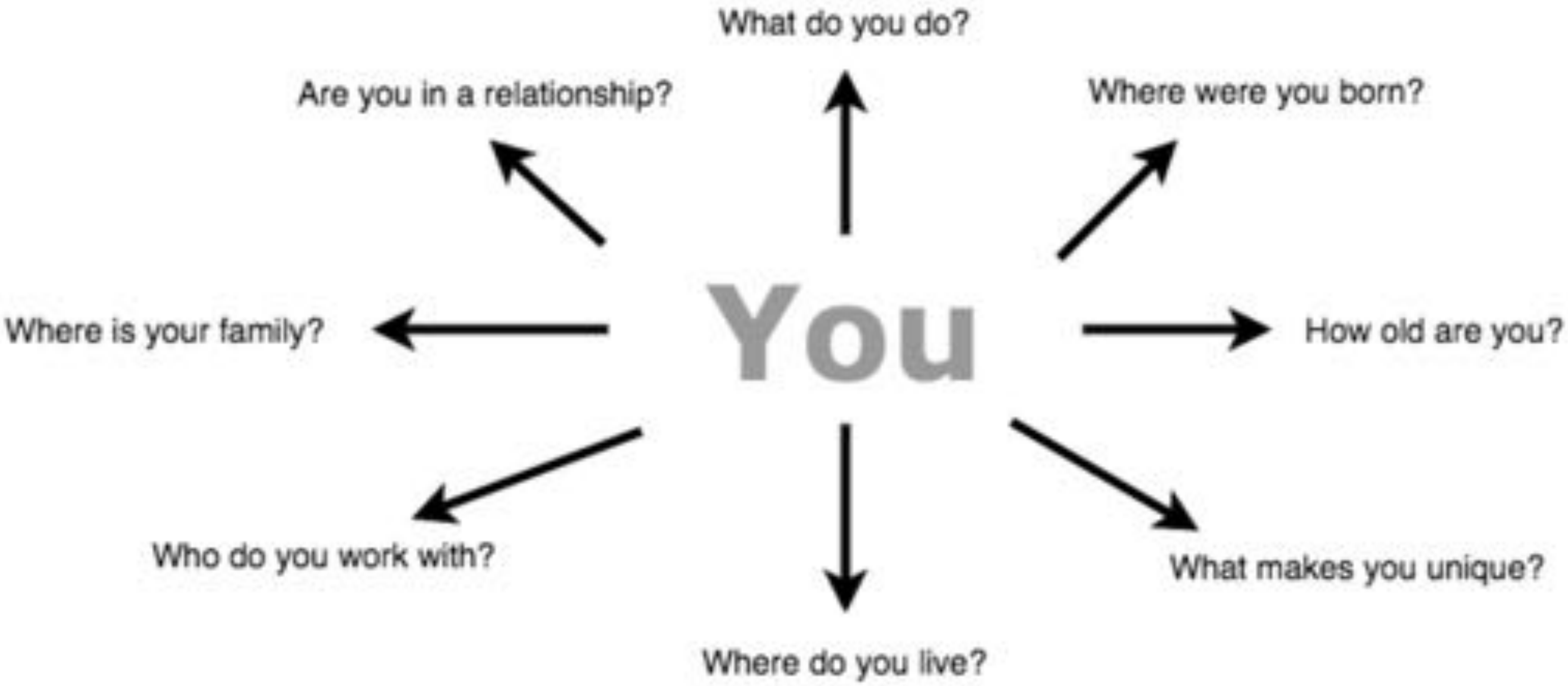
107.183.243.182

Marcus@mail.g00gle.bid

f43cf95a5b19f48a9dff32d518b395dc

History

All those bits of data that tell us about you



- Nicholas Sparks rolled out this beautiful saying that I often butcher, but like to use nonetheless

“Nothing is ever lost nor can be lost…”.

- The “H” in CHRIME is about history, specifically the history of the element you are examining with CHRIME and those elements linked to it.
- History and reputation tend to be intermingled a lot, but it is key to remember that we specifically mean the Who, What, Where, and When here.

What? So What? Now What?

- Also called the ladder of inference (W^3)
- Its a line of reflective questioning to tease out important history elements.

- From your fact pattern (Constellation) you ask:
  - WHAT?
  - What happened?
  - What was noticed, what facts or observations stood out?”

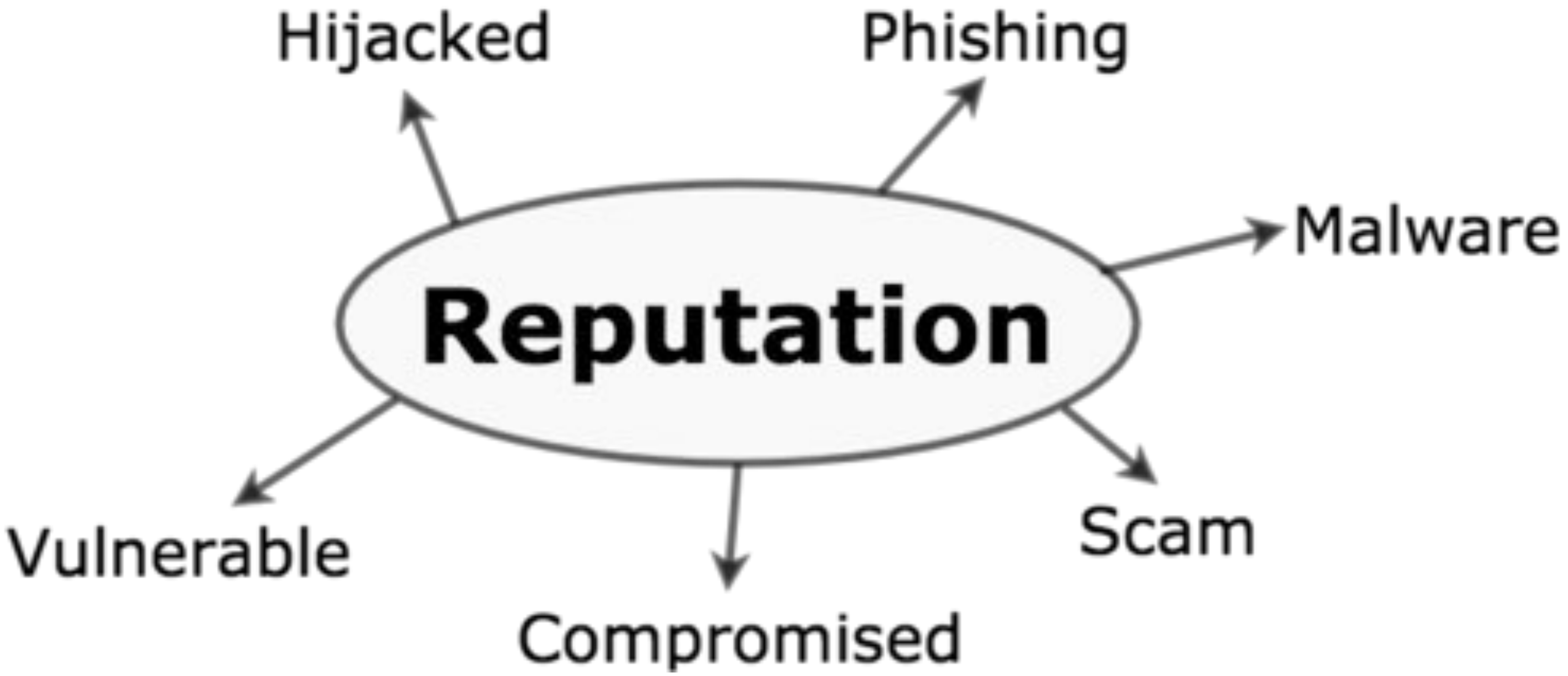
- After all the salient observations have been collected ask:

  - Why is that important?
  - What patterns or conclusions are emerging?
  - What hypotheses can be made?”
- This line of inquiry helps make sense out of the information. Finally, after making sense of things you ask, “NOW WHAT? What actions make sense at this point?”

History exercise

Perform the History steps for previously built Constellations.

What everyone thinks about you

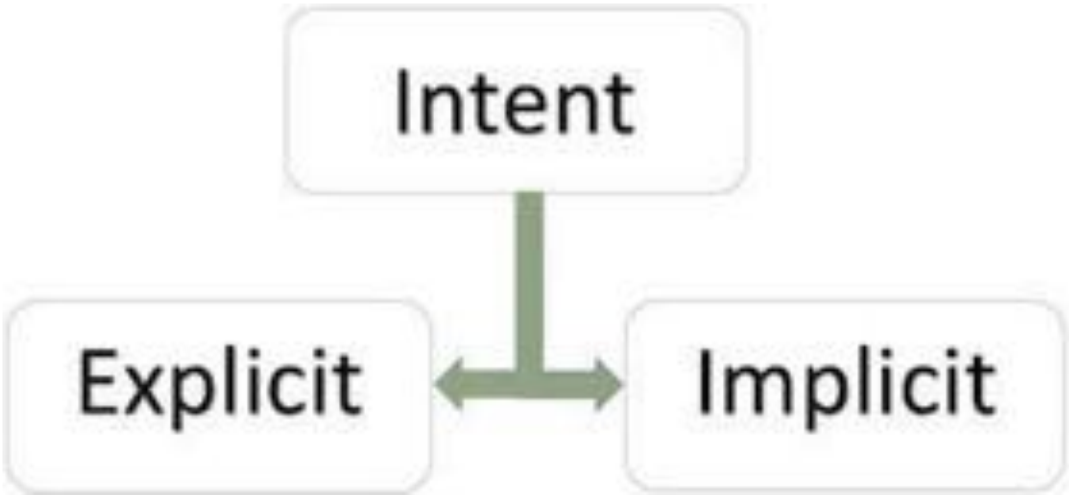


- Usually done together with (H)istory since the checks are very similar.
- Reputation cares about how you have said about the data
- Also, what other reputation sources have said about the data

Sidebar on Solr

Reputation exercise

Starting point
ccgonzalezmoreno.com.ar



Intent

Explicit

Implicit

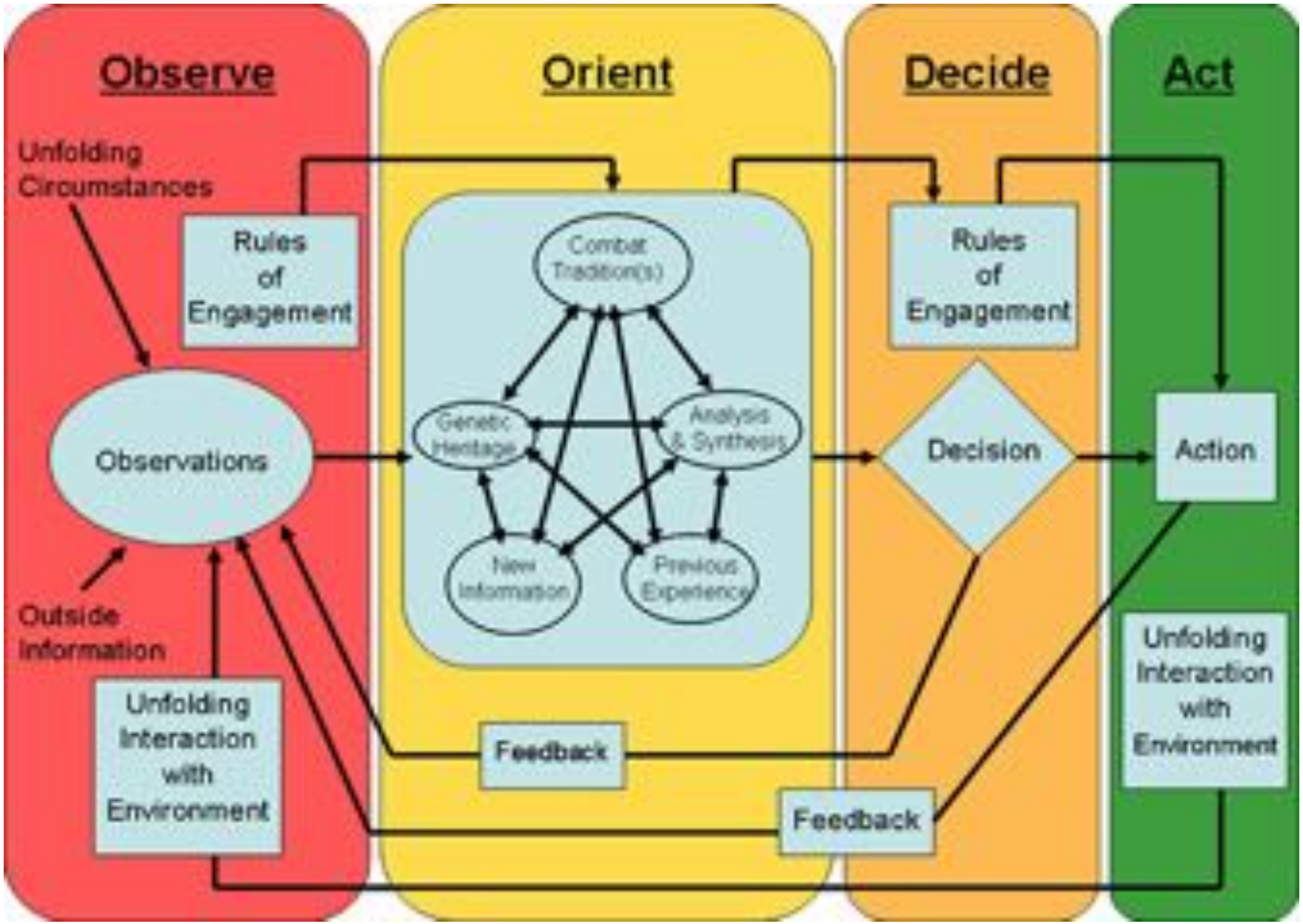
The purpose, direction or goal. It might be logical or only something inferred from context, existence or usage.

Our intention creates our reality

- It’s all about attention, or resolve if you prefer.
- It’s equally a discussion of focus and the point behind performing an action.
- It speaks to the “why”, something always asked in the context of an event.
- After all, who hasn’t, as an intelligence analyst, been asked the question of “why did this happen?”, or “why did they attack us?”. Intent also applies to the other side of the attack wheel. Why did the adversary take a specific action or why did a series of events happen in the particular order observed?
- It’s intent that defines that course of thought.

- CHRIME demands you define intent for the simple reason that you are going to do so anyway and it should be a planned activity if it’s going to happen.
- Intent will be a question asked, either from you, the analyst, or the person who requested the action.

Sidebar on temporary intent


Observe
Orient
Decide
Act
Unfolding Circumstances
Rules of Engagement
Observations
Outside Information
Unfolding Interaction with Environment
Combat Tradition(s)
Genetic Heritage
Analysis & Synthesis
New Information
Previous Experience
Rules of Engagement
Decision
Action
Feedback
Feedback
Unfolding Interaction with Environment

Intent exercise

This domain was previously blocked. Is it currently safe to remove the block?

goquick-mind.asia

- Malware is a defined variable in the equation of making a decision.
- Unlike HRI of CHRIME, Malware is not inferred; it either exists or doesn’t.

“M” stands for Malware

- A point of caution comes is in order.
- The absolute initial step for the “M” in CHRIME is to outline the communication, composition, function, organization of the malware.
- This is the Tier-I action that constitutes the first look at the malware. Outline what you can, label that as confidently as possible and be ready to be wrong — at least, some of the time. The potential for incorrectness is why malware is not a sole information collection and correlation step.
- A lot of intelligence can be derived from malware and related files, but it cannot stand alone.

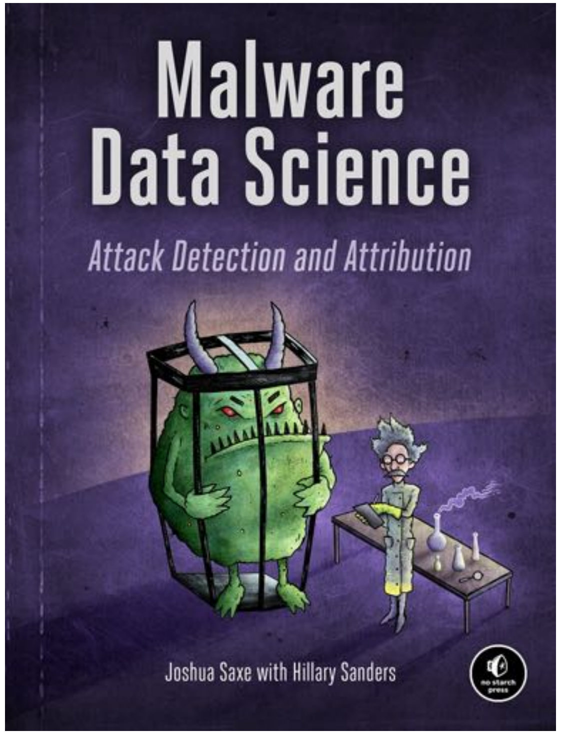
- It needs other data and correlation to be functional.
- The next bit, if needed to reach the decision point, is deeper detail.

Sidebar on more detailed analysis

- Go for accuracy and make sure what you have outlined is correct. That means research, investigation and probably reverse engineering, or at least file interrogation. The last step is to attribute.

- Attribution is building a case of circumstantial and incomplete data. It should be done with the thought that the best lawyers in existence are going to challenge every single piece of evidence, no matter how insignificant or compelling.

Sidebar on Malware Attribution


Malware Data Science
Attack Detection and Attribution
Joshua Saxe with Hillary Sanders
no starch press

- Go for accuracy and make sure what you have outlined is correct. That means research, investigation and probably reverse engineering, or at least file interrogation. The last step is to attribute.
- Attribution is building a case of circumstantial and incomplete data. It should be done with the thought that the best lawyers in existence are going to challenge every single piece of evidence, no matter how insignificant or compelling.

- The tie-up activity, even if you skip deeper detail and attribution, is always to correlate the malware to the event.
- You have malware. The need to understand how it correlates and fits (or doesn't) in the event is critical.
- If the malware doesn't belong to this event, then it belongs to a different one — an event you hopefully knew about and just missed the connection.
- Otherwise, the string comes back to a python that can entangle and strangle you to death as you explain why it was missed and what damage happened on your watch that you missed.
- Someone's head usually rolls in that situation. That's an ugly and unpleasant discussion to be avoided whenever possible.

TIME FOR
ACTION
TIME FOR
X

- Execution comes last in CHRIME, but it’s far from the end at the same time.
- Like I’ve mentioned more than once, it can be the beginning, where the steps of the operation performed are a better starting point.
- I’ve highlighted many times that CHRIME is meant to be flipped or even used in portions to meet your needs. That is part of its allure and agility, that it can function so flexibly.

ACTION

Execution exercise

Phishing email to end point infection example

CHRIME recap

- Shorthand for a technique to get to 80% complete answers as quick as possible.
- Goal is always "just enough" information to sway the decision but also enough for sufficient, repeatable documentation.

Files and Slides

https://github.com/CyberDefenses/Conventions

Questions?

Twitter:	@montystjohn
LinkedIn:	www.linkedin.com/in/monty-st-john-3842692
Github:	github.com/corumir
CDI Github:	github.com/cyberdefenses