Getting Intelligence Right

Delivering trustworthy intelligence by operationalizing Intelligence Management
September 16th, 2021

Agenda

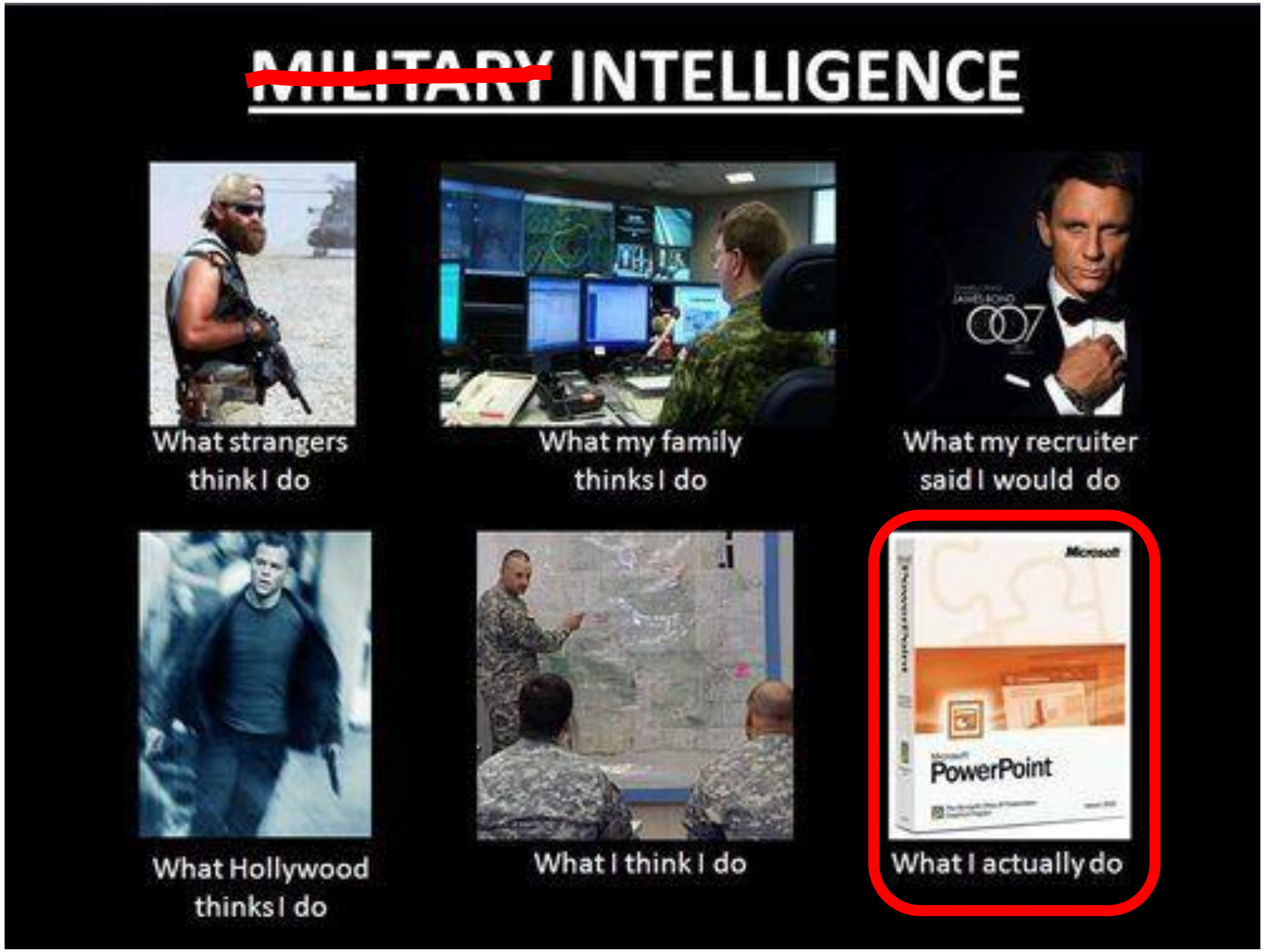
– Everyone has one

- WhoAmI
- Definitions, because words matter
- Intelligence Cycle
- Intelligence Management
- How NFCERT does intelligence
- Where does trust come from?
- Mind Map (if time)
- Q&A

WhoAmI

– That's All I'll Ever Be

- Freddy Murre
- Senior Threat Intelligence Analyst @ NFCERT
- BA in Marketing and HR
- MA in Counter Terrorism
- MA in Intelligence


~~MILITARY~~ INTELLIGENCE
What strangers think I do
What my family thinks I do
What my recruiter said I would do
007
What Hollywood thinks I do
What I think I do
Microsoft PowerPoint
What I actually do

Worlds Colliding

– A Better One is Created

- Cyber Security
- Business Interests (Risk)
- Intelligence (Process)

By structuring your intelligence production, you will firstly make sure that the **most important needs are met** and this build trust. Secondly, that the work you do is **streamlined towards meeting those requirements**.

Words Matter (aka Definitions)

– Choose Them Carefully

- Threat
- Intelligence

A threat is the human behind the keyboard, it’s the entity involved in the execution of an intrusion”

(Robert M. Lee - SANS FOR578)

Words Matter (aka Definitions)

– Choose Them Carefully

- Threat
- Intelligence

- “Any **contextual** and **processed** information and **knowledge** about a past, ongoing, or upcoming incidents, that is processed and assessed by a **human**”

and

- “that provide **answers** to information gaps and provide **decision support** in a **timely** manner”

(NFCERT)

Words Matter - Data – Information – Knowledge – Intelligence

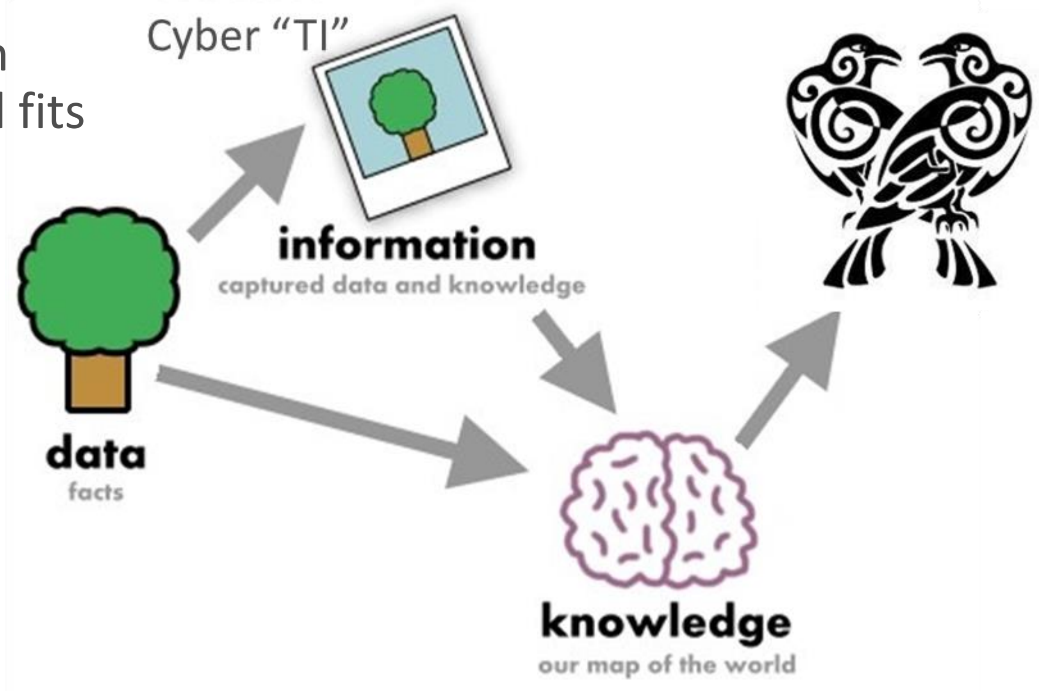
– Choose Them Carefully

Data vs Information vs Knowledge vs Intelligence

- **Data/IOC**: An internal IP address observed communicating to an external IP or domain.
- **Information**: The IP address in context, i.e. the IP connects from internal HW to an external, known C2 network (Diamond model fits here)
- **Knowledge**: The IP address has also been observed hosting different domains in other malicious campaigns. The recipient of the malicious email that launched the malware is on a known mailing list from a known source.
- **Intelligence**: When an analyst looks at the data and information and uses his/her knowledge to provide assessments in order to answer **information gaps** and provide **decision support**.

Vendors:
Cyber "TI"

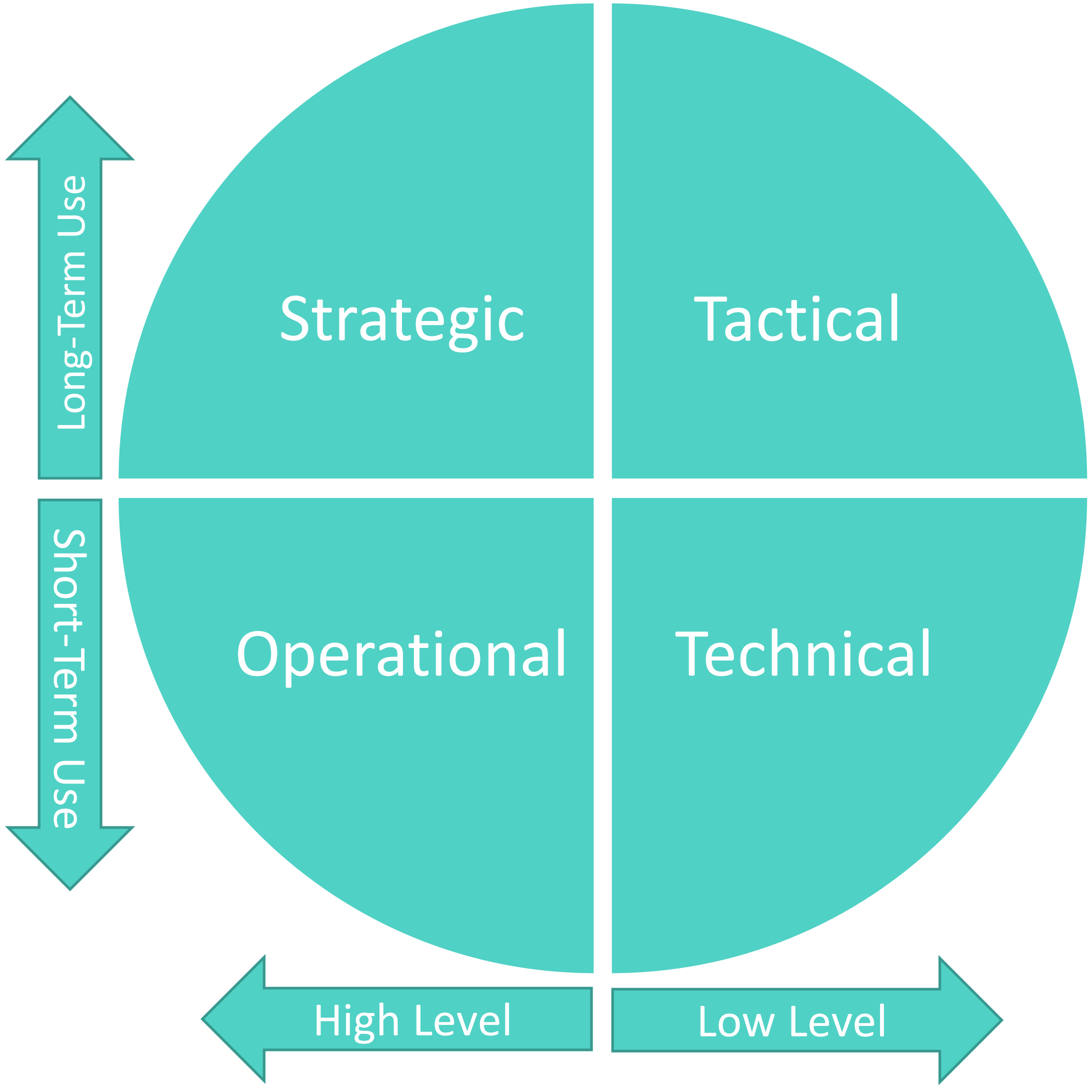
IOCs



Words Matter (aka Definitions)

– Choose Them Carefully

- Strategic
- Operational
- Tactical
- Technical



Levels

– On a level, far, far away

- Determines the consumer's "time available"
  - Example: strategic level may have less time than technical.
- Provides guidance on the amount of details
  - Too much and it will not be understood or even read by a strategic consumer.
- Provides input to the "Analytic Spectrum"

Levels

– On a level, far, far away

- **Political:** Mostly out of scope, supporting government entities, FSA’s, NCSC’s, etc.

- **Strategic**: High-level information and intelligence on changing risk. Goal is to inform business decisions and used to set relevant priorities. Has a **long-term** focus, often contains attribution, consumed at **board level** or by other **senior decision-makers** and **stakeholders** at the business leadership level.

- **Operational**: Contains information about campaigns, attacks, events in progress or impending attacks against one or more NFCERT member. Also contains actor's **Modus Operandi** (different TTPs over time), capabilities, intentions and motivations of adversaries. Initially consumed by defenders and higher-level security staff, such as **security managers** or heads of incident response.

Levels

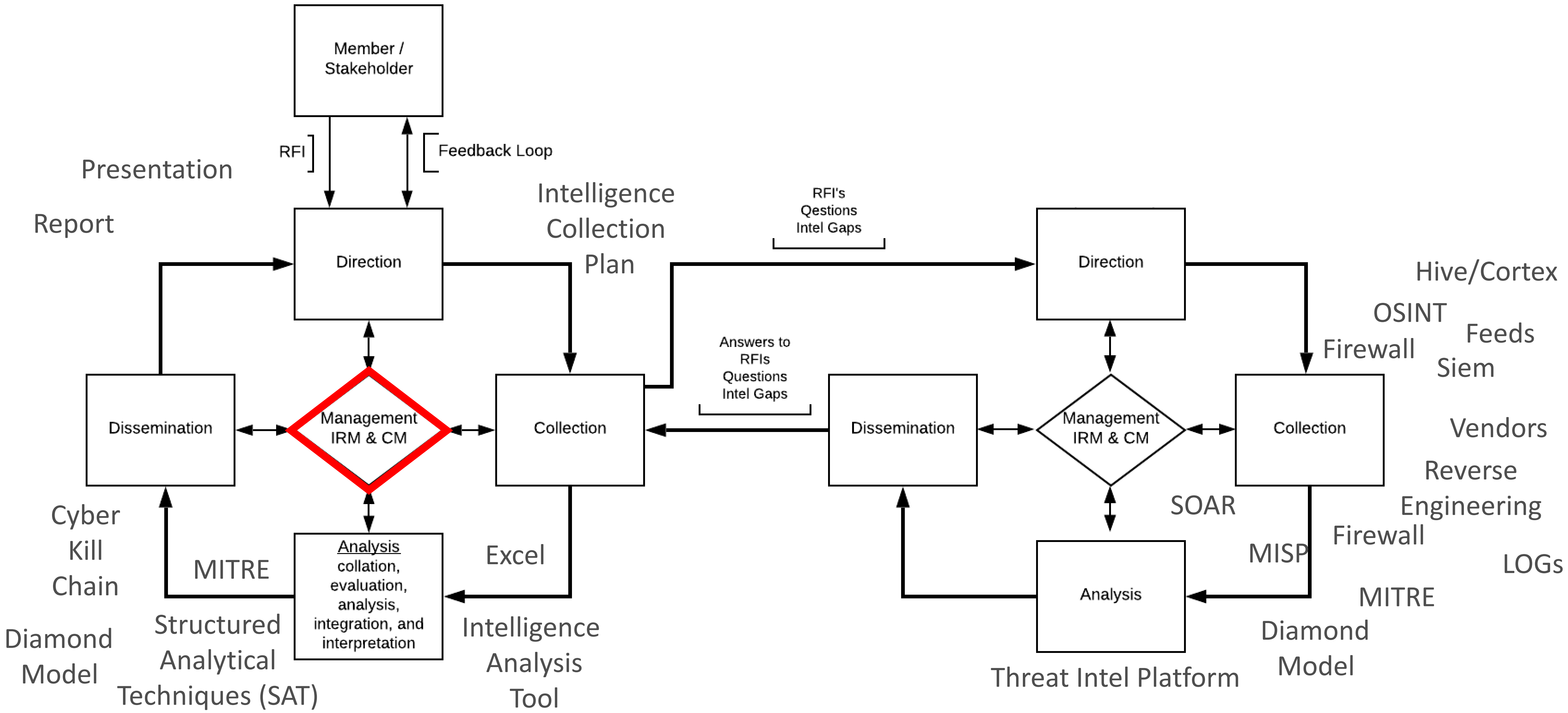
– On a level, far, far away

- **Tactical**: Contains attacker's methodologies, tactics, techniques and procedures (**TTPs**), mapped to MITRE ATT&CK, and is information about how adversaries are conducting attacks, who they are, how they are organized, etc. Often consumed by **security staff**, security **analysts**, system **administrators** and **architects.**

- **Technical**: Focus on indicators of compromise (**IOCs**), tools, and artefacts. Little-to-no contextualization or learning. Often consumed by **SOC staff** and **incident responder**, and shared through technical means, such as MISP.

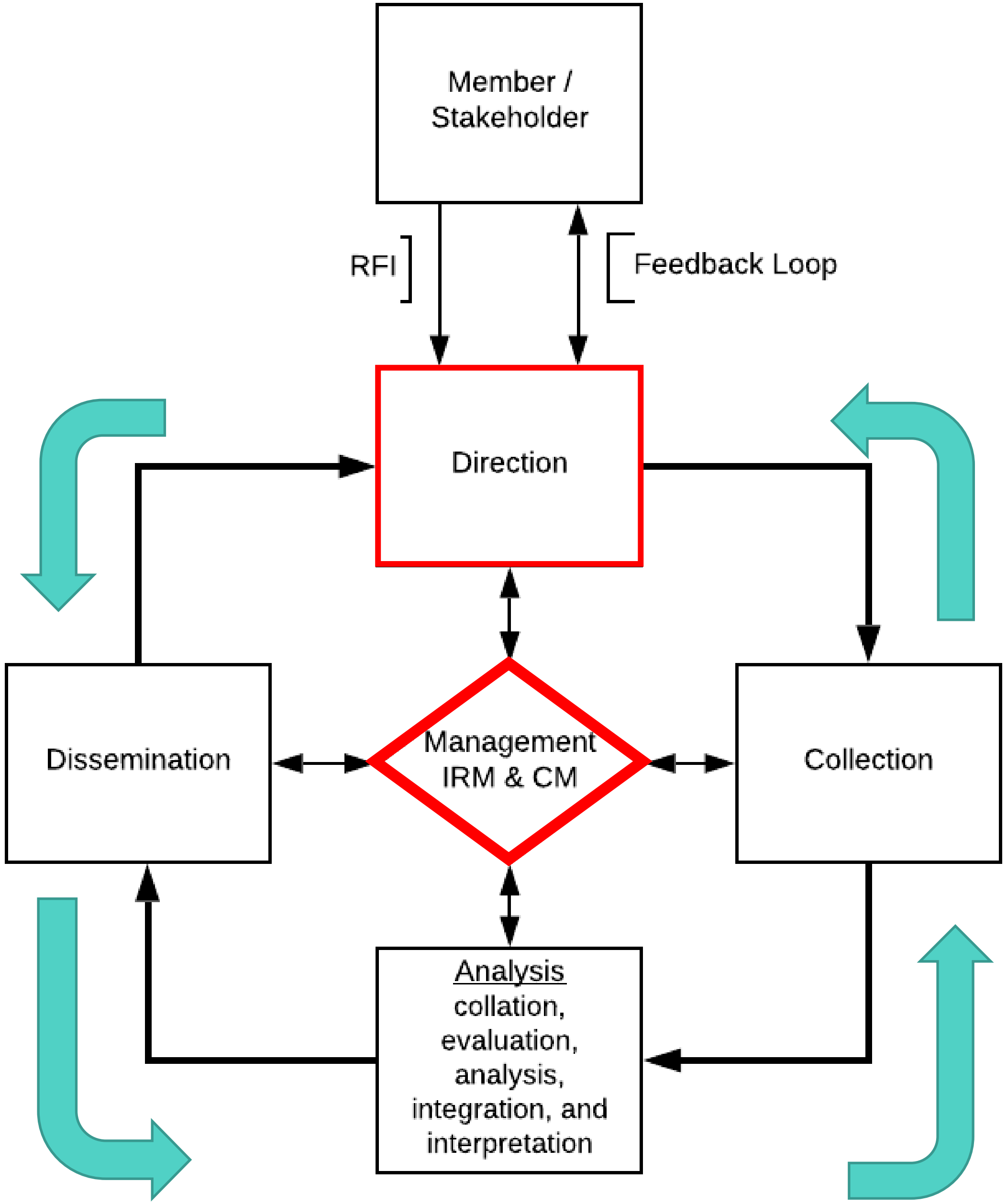
Intelligence Cycle (Strategic ← → Technical)

– Oh Why Do You Hate It So



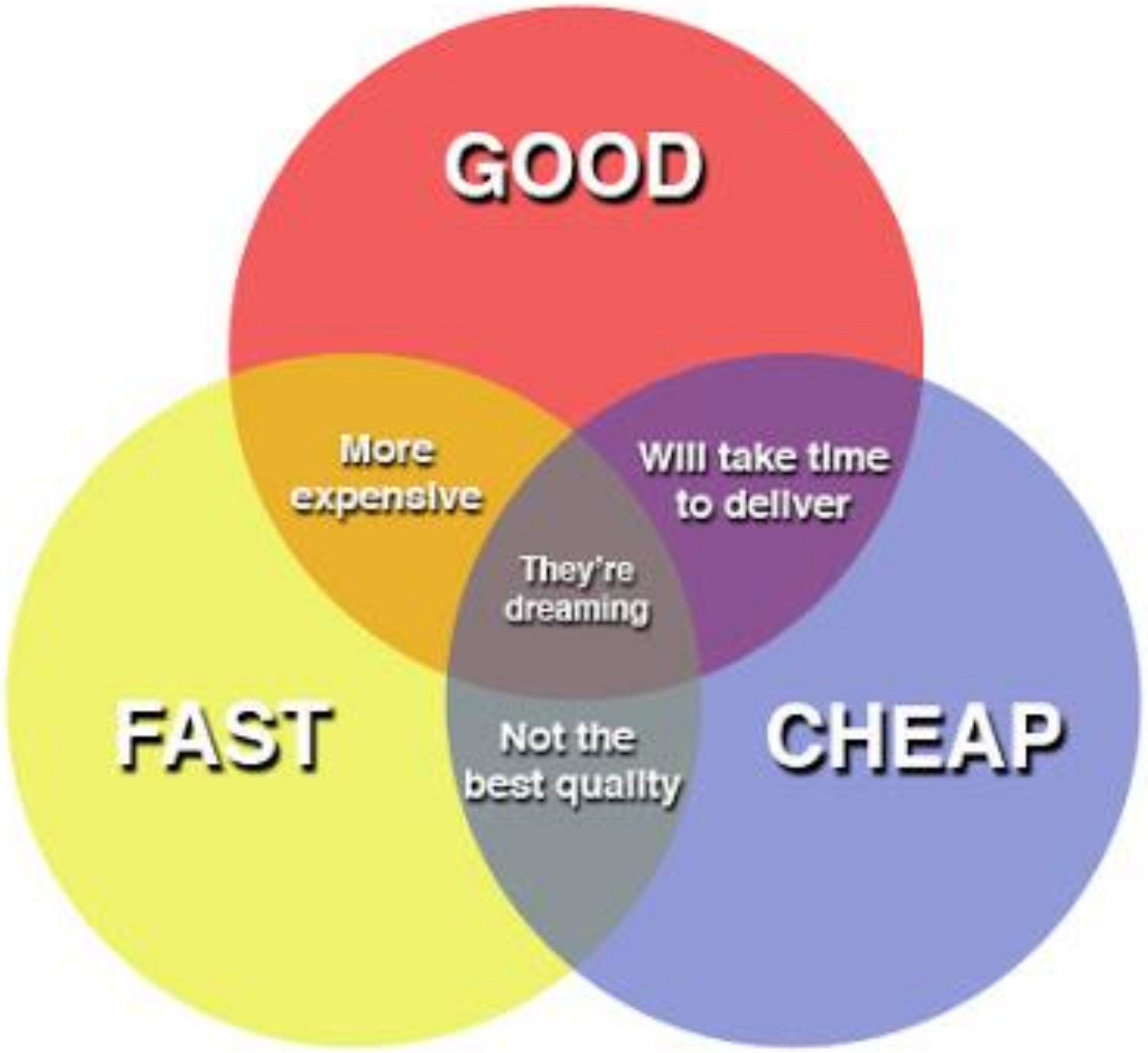
5W+H

- Who are the stakeholder(s)?
- What do they ACTUALLY want to know?
- Why do they want it?
- When do they want it?
- What type of product do they want?
- How do they want it delivered?



5W+H

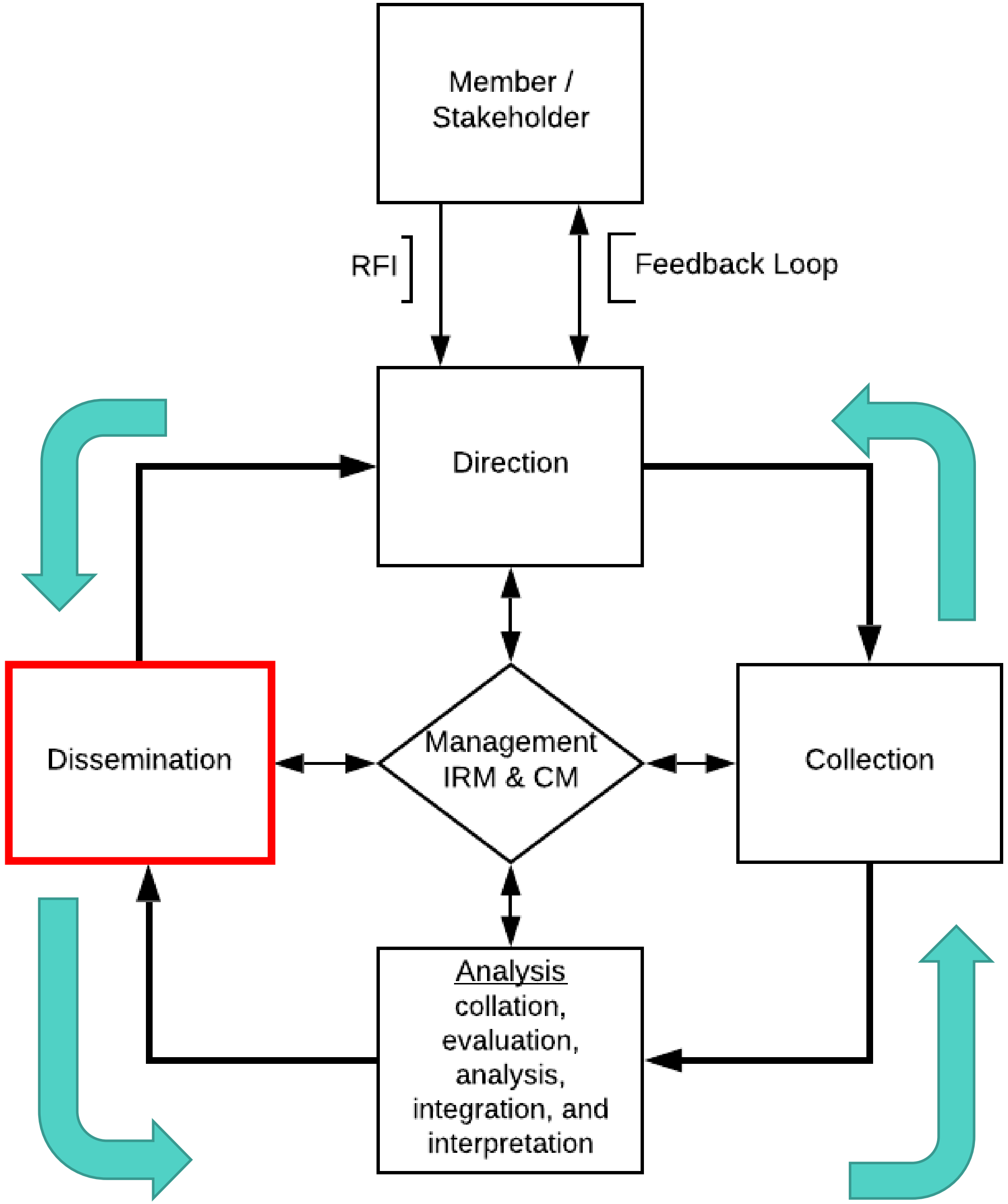
- Who are the stakeholder(s)?
- What do they ACTUALLY want to know?
- Why do they want it?
- When do they want it?
- What type of product do they want?
- How do they want it delivered?



Level

- What is the level of the stakeholder(s)?
    - Strategic
    - Operational
    - Tactical
    - Technical
- How much time do they have?
- What detail level do they like

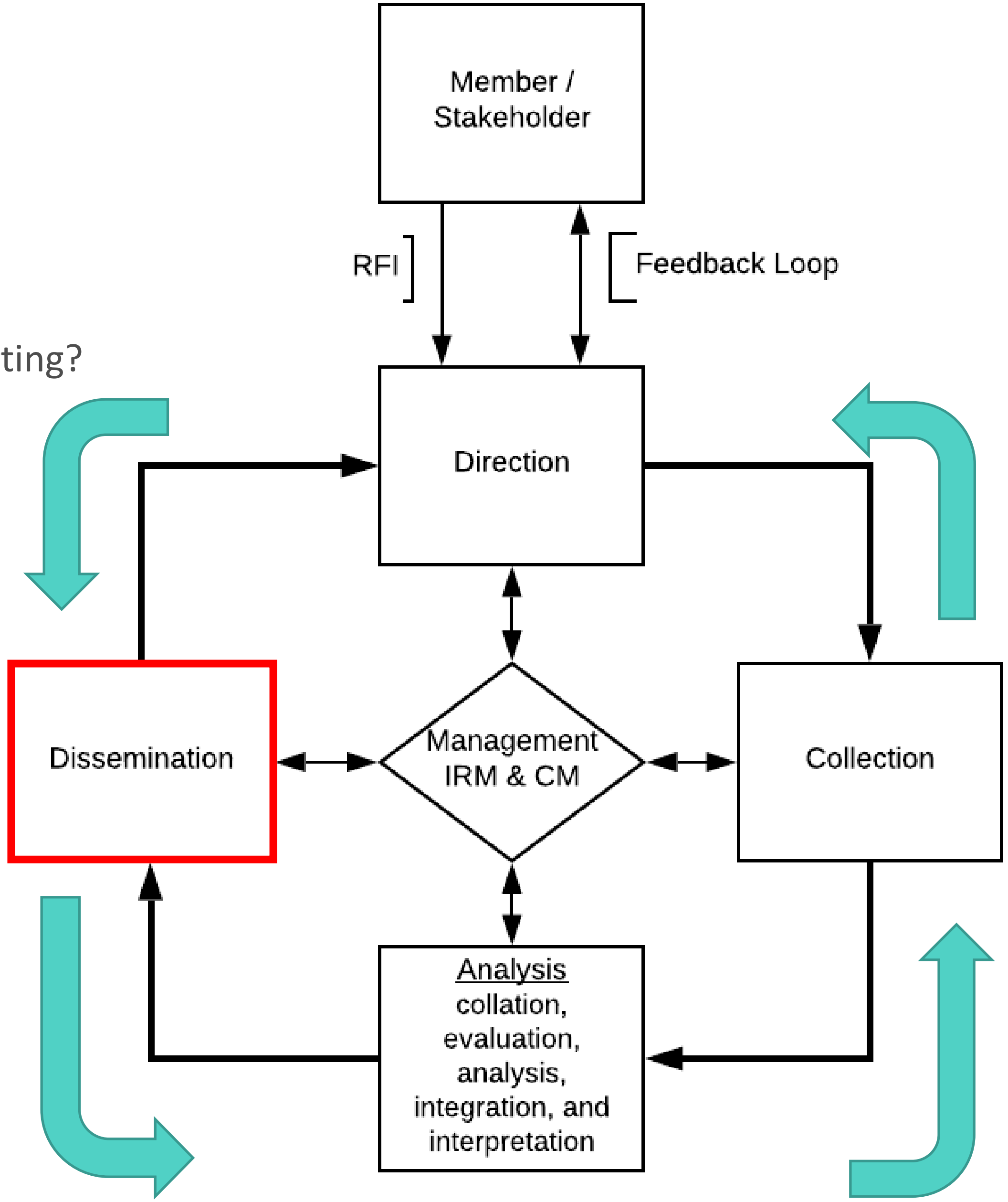
= Input to Product



Decision

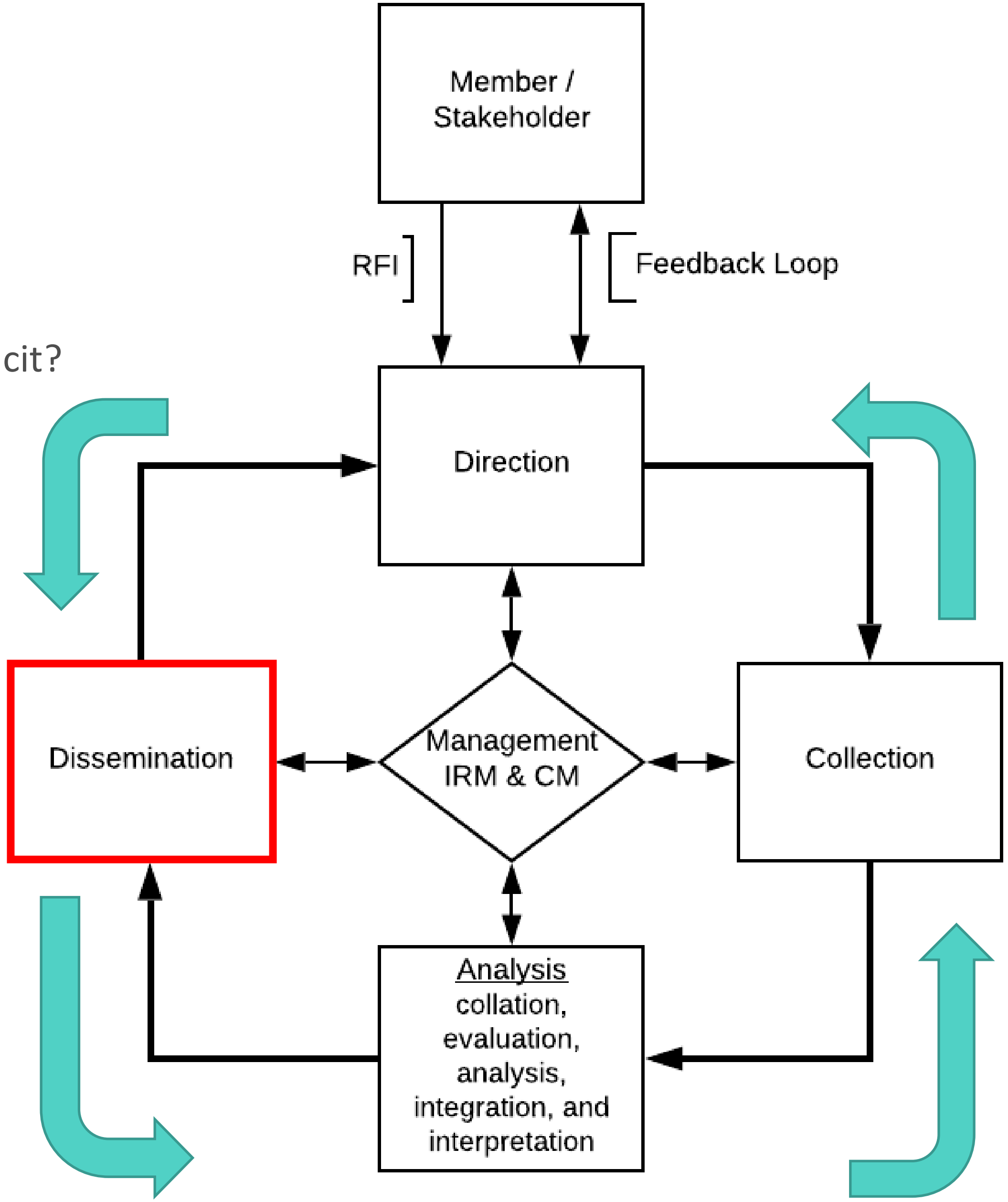
- What are the decision(s) we are supporting?

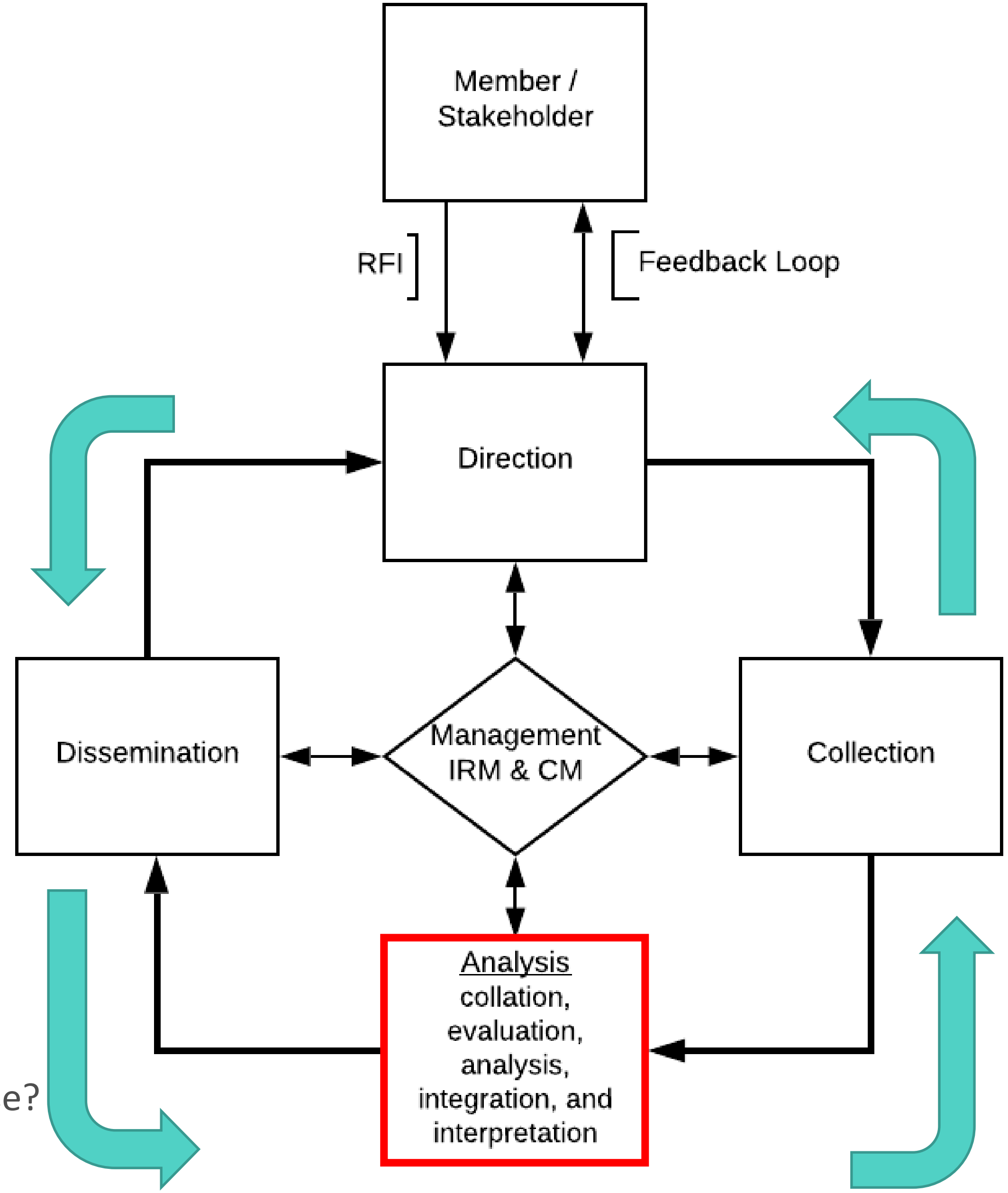
= VALUE!!!



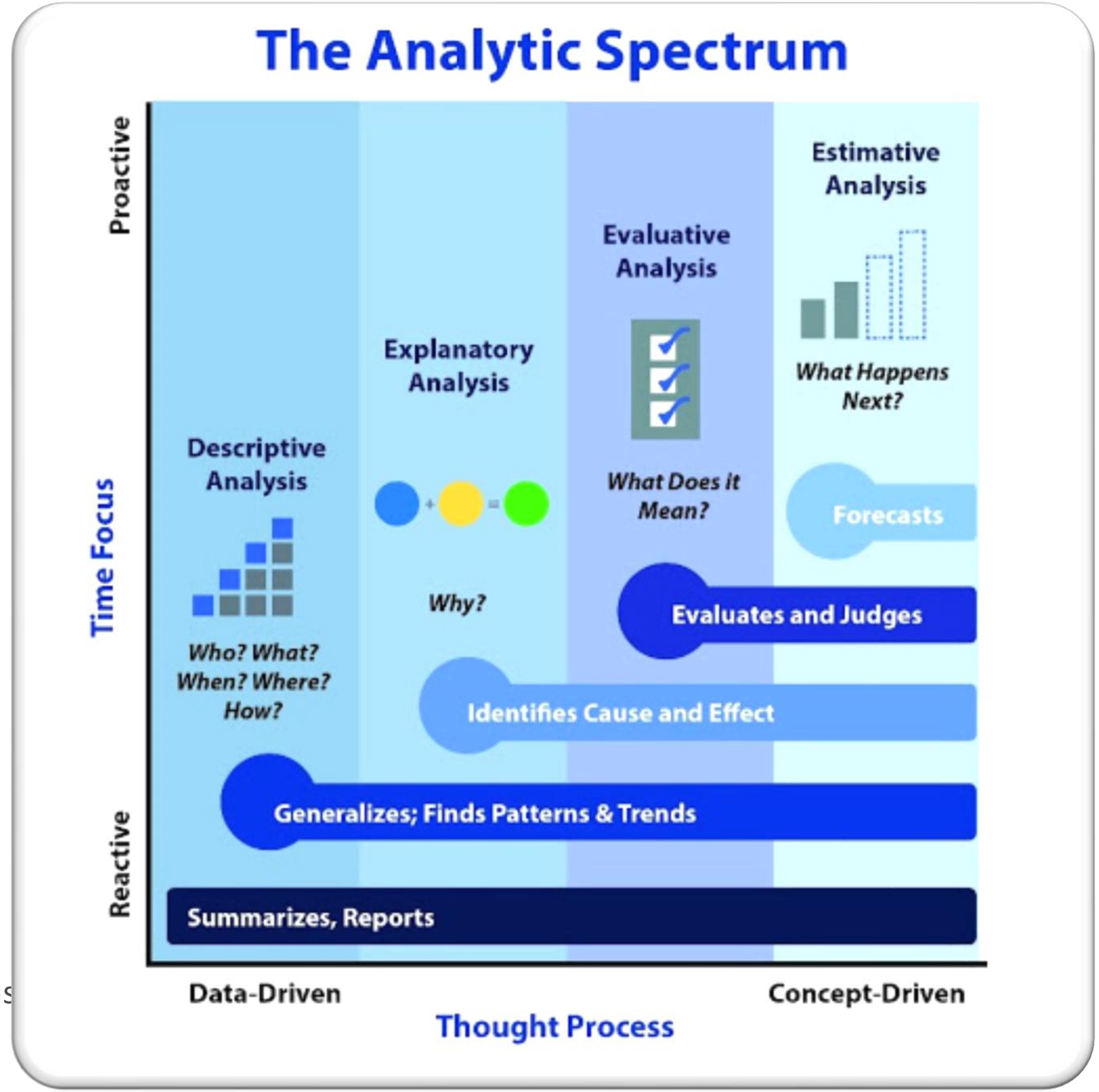
Boundaries

- Which boundaries are explicit and implicit?

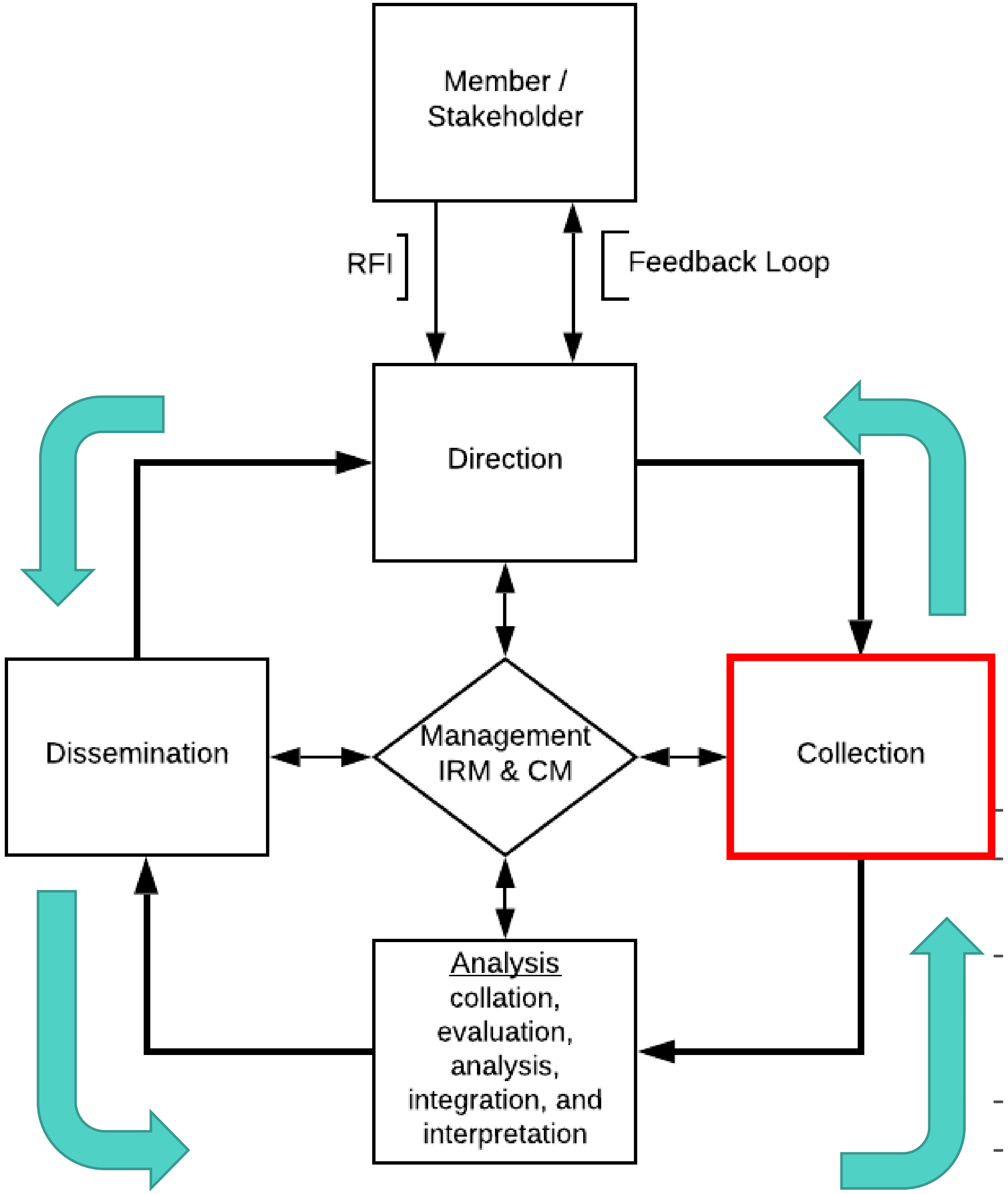




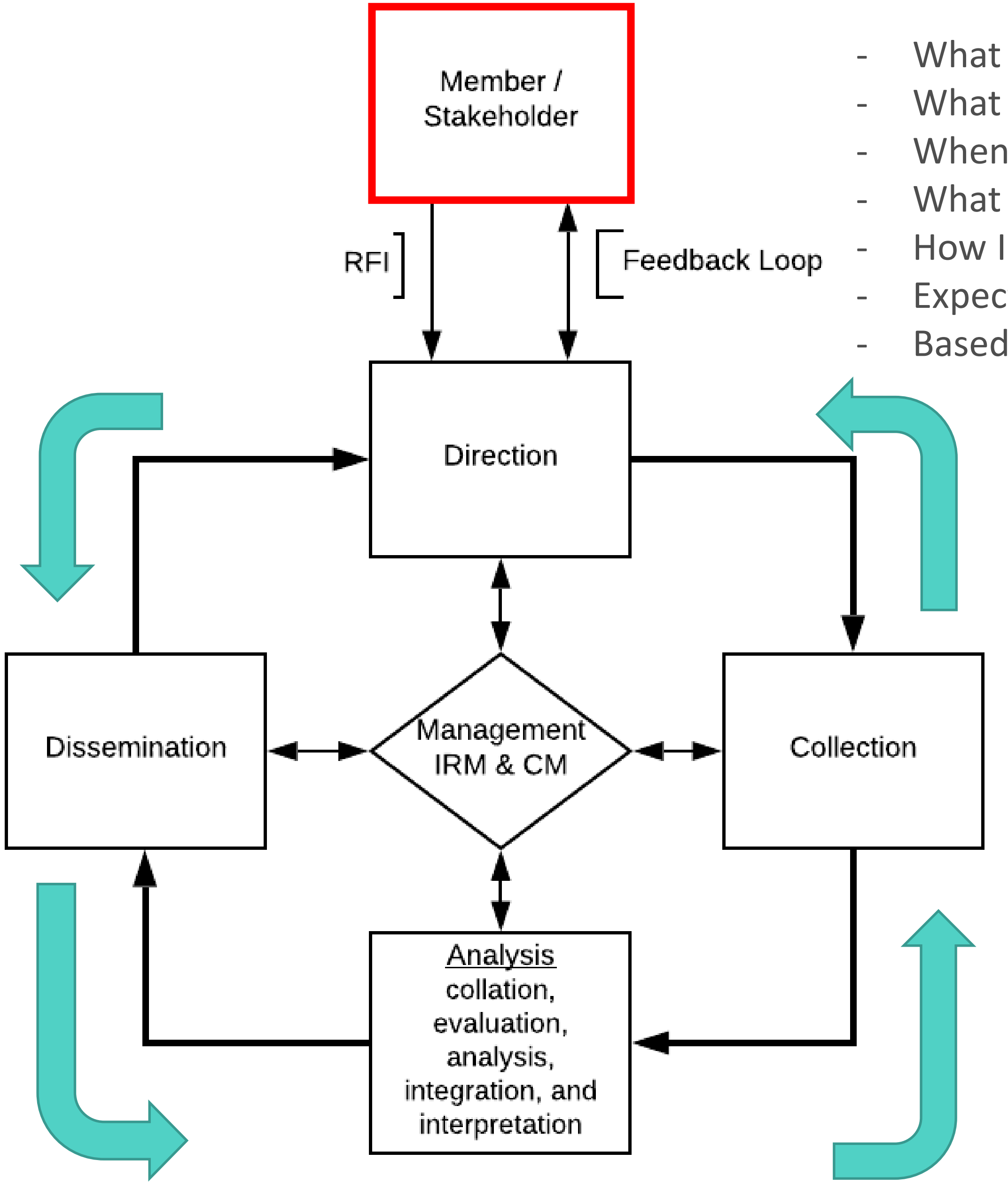
- What type of analysis are we doing?
- Which combo of SATs are we using?
- Which type of tools should we use?
- Which cyber intel models should we use?



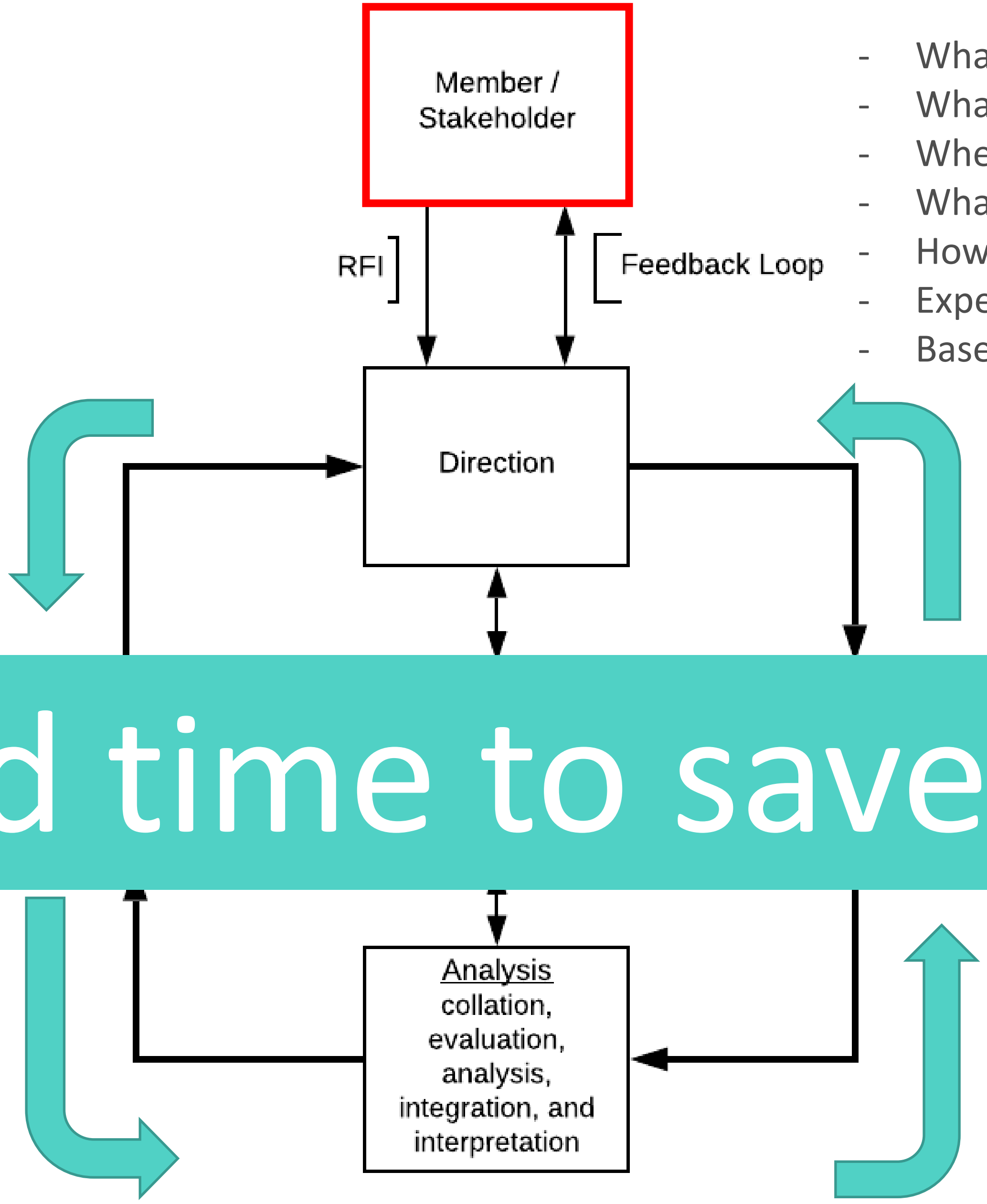
- What type of analysis are we doing?
- Which combo of SATs are we using?
- Which type of tools should we use?
- Which cyber intel models should we us



- Check basic intelligence
- What do we know/not know?
  - Discover Intel gaps
- Where to collect from?
  - Do we have access?
  - Do we have to develop access?
- Who will collect it?
- How long will it take?



- What stakeholder(s) wants to know, rephrased
- What function/process we are supporting
- When the stakeholder(s) wants it
- What type of product stakeholder(s) wants
- How I will work through the steps
- Expectations & Metrics Management
- Based on feedback, make adjustments


Member / Stakeholder
RFI
Feedback Loop
Direction
Analysis
collation, evaluation, analysis, integration, and interpretation

Spend time to save time

- What stakeholder(s) wants to know, rephrased
- What function/process we are supporting
- When the stakeholder(s) wants it
- What type of product stakeholder(s) wants
- How I will work through the steps
- Expectations & Metrics Management
- Based on feedback, make adjustments

Stakeholder Engagement

– the key to your analysis

- A stakeholder is anyone who has any interest/influence in what you are doing
- Stakeholders will determine the success, or not, of your projects and activities

Stakeholder engagement contains several steps:

1. Identify who your stakeholders are
2. Analyze your stakeholders to gain insights
3. Plan how you will engage with them to meet your objectives
4. Act on your plans, and handle any feedback you encounter
5. Review progress and re-engage to make further progress

Intelligence Requirement (IR) Analysis

– the window to their soul

We always do it to:

- Reduce/minimize intelligence failures (value)
- Address the correct needs of the stakeholder/consumer (value/effectiveness)
- Identify the issue/topic of importance (effectiveness)
- Use the right tools and techniques (effectiveness)
- Prioritize our Intelligence Requirements (IRs) and resources (effectiveness)
- Identify knowledge gaps and new IRs (Value)

Acts as input to:

- Intelligence Requirement Management (IRM)
- Intelligence Collection Management (ICM)

Improving effectiveness:

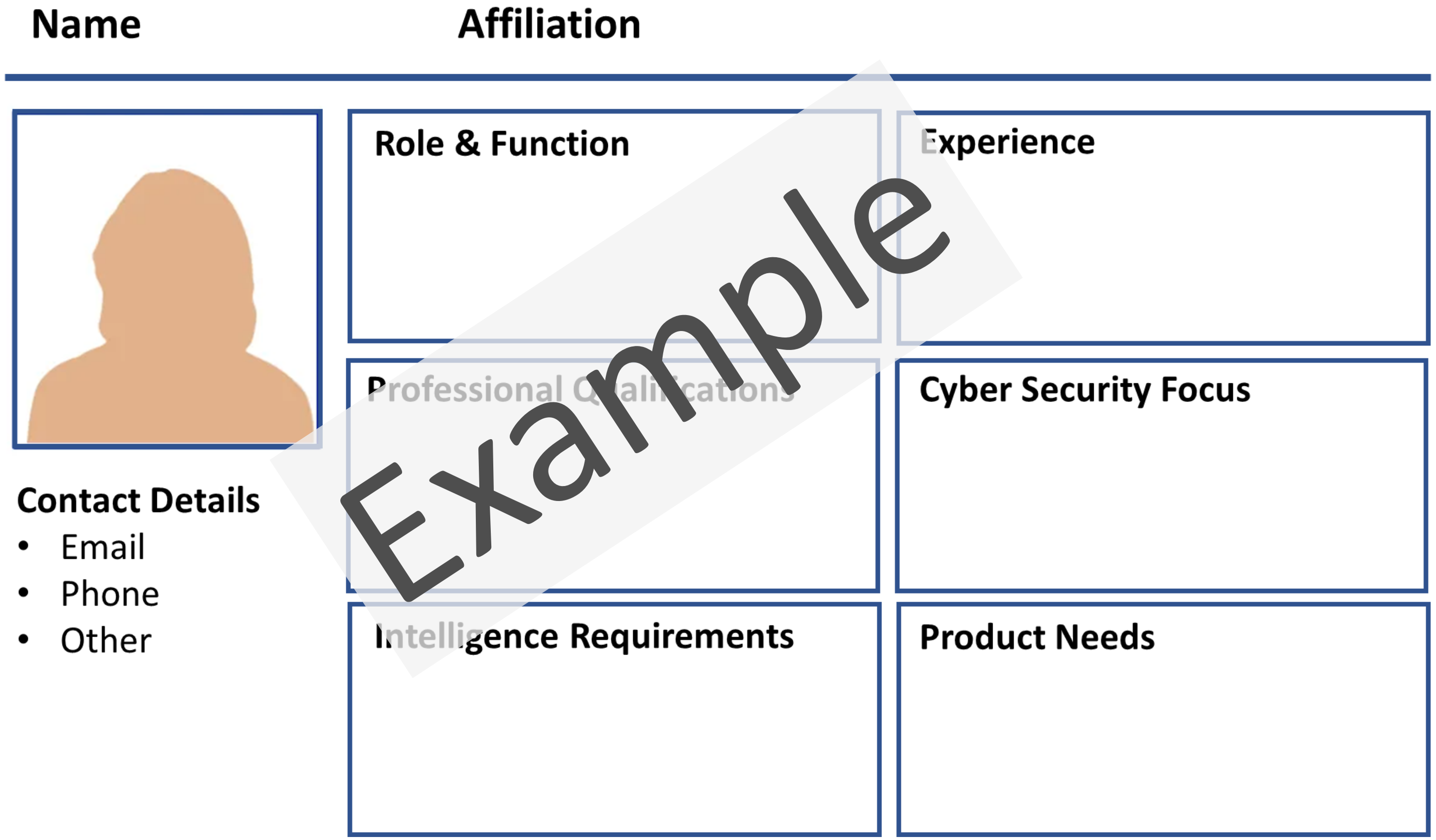
- Focus on the right “thing”
- Use the right tools and techniques

Stakeholder Cards

– Improve your game

Should include

- Role and function
- Experience
- Professional Qualifications
- Their IT-Sec focus
- Product needs
- Intelligence Requirements



Name **Affiliation**

Role & Function

Experience

Professional Qualifications

Cyber Security Focus

Contact Details

- Email
- Phone
- Other

Intelligence Requirements

Product Needs

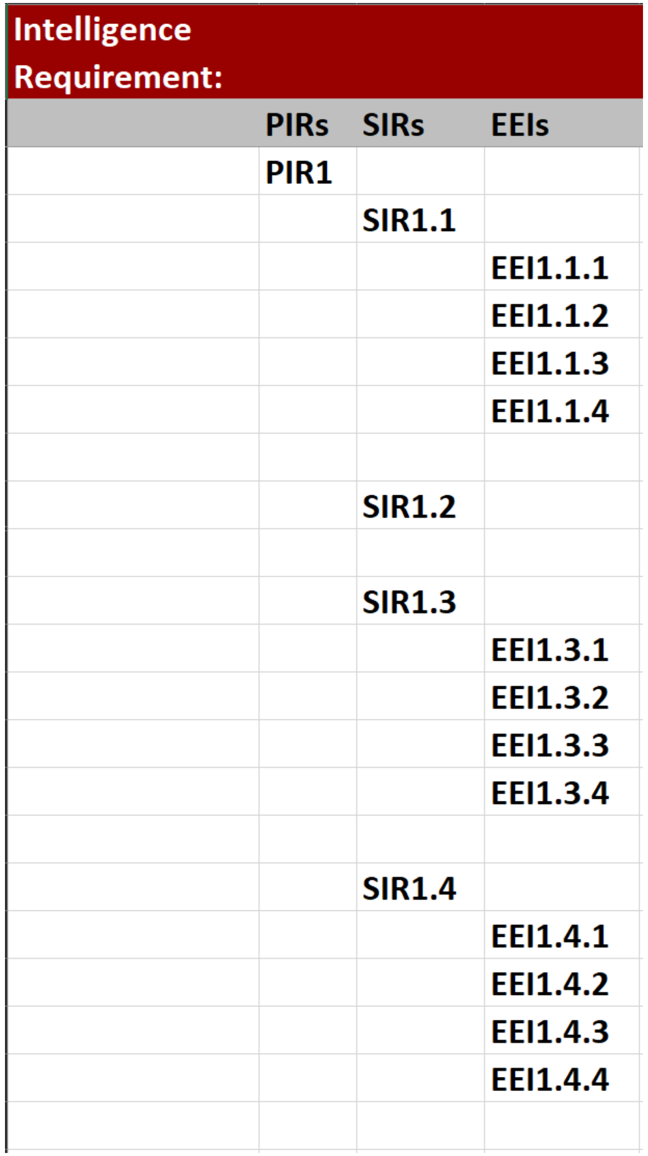
Intelligence Requirements

– Without It You Are Blind

Intelligence Requirements are the objectives an analyst seek to satisfy through the intelligence process, or, “a knowledge gap that needs addressing to enable decision”.

Best practice:

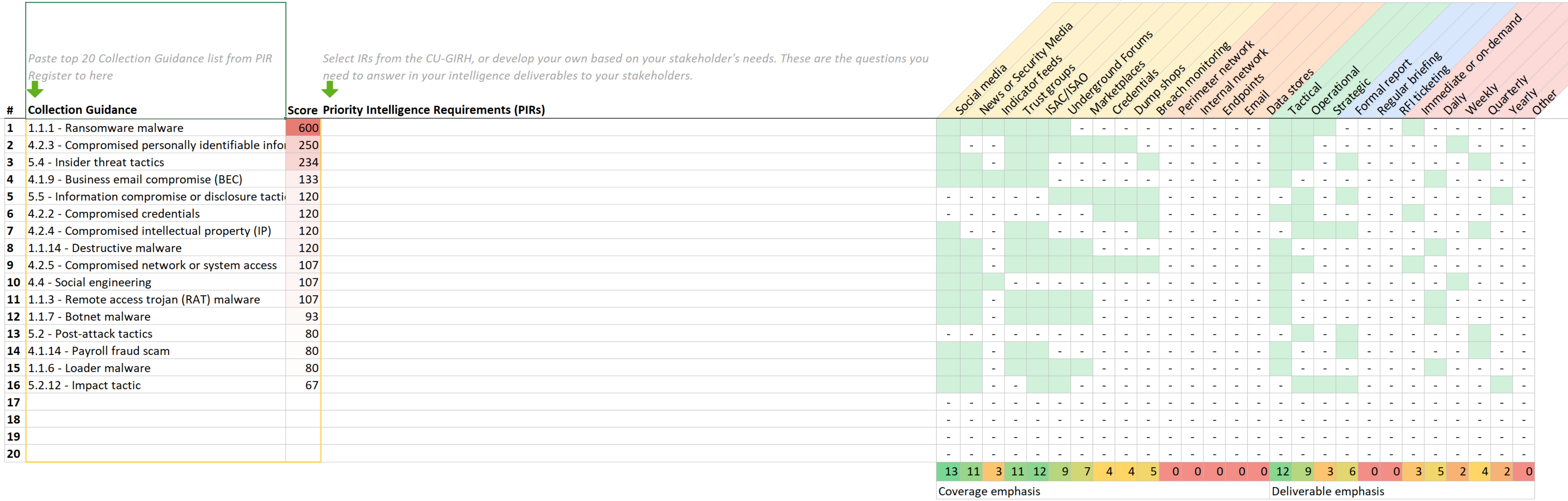
- Ask only one question
- Support a single decision
- Prioritized Intelligence Requirement (PIR)
- Specific Intelligence Requirement (SIR)
- Essential Elements of Information (EEI)



Intelligence Requirement:			
	PIRs	SIRs	EEIs
	PIR1		
		SIR1.1	
			EEI1.1.1
			EEI1.1.2
			EEI1.1.3
			EEI1.1.4
		SIR1.2	
		SIR1.3	
			EEI1.3.1
			EEI1.3.2
			EEI1.3.3
			EEI1.3.4
		SIR1.4	
			EEI1.4.1
			EEI1.4.2
			EEI1.4.3
			EEI1.4.4

Intelligence Requirements Management (IRM)
Intelligence Collection Plan (ICP)

https://intel471.com/resources/cu-girh-download-request



Paste top 20 Collection Guidance list from PIR Register to here

Select IRs from the CU-GIRH, or develop your own based on your stakeholder's needs. These are the questions you need to answer in your intelligence deliverables to your stakeholders.

#	Collection Guidance	Score	Priority Intelligence Requirements (PIRs)	Social media	News or Security Media	Indicator feeds	Trust groups	ISAC/ISAO	Underground Forums	Marketplaces	Credentials	Dump shops	Breach monitoring	Perimeter network	Internal network	Endpoints	Email	Data stores	Tactical	Operational	Strategic	Formal report	Regular briefing	RFI ticketing	Immediate or on-demand	Daily	Weekly	Quarterly	Yearly	Other
1	1.1.1 - Ransomware malware	600		🟩	🟩	🟩	🟩	🟩	🟩	-	-	-	-	-	-	-	-	-	🟩	🟩	🟩	-	-	-	🟩	-	-	-	-	-
2	4.2.3 - Compromised personally identifiable infor	250		🟩	-	-	🟩	🟩	🟩	🟩	🟩	🟩	-	-	-	-	-	-	🟩	🟩	-	-	-	-	-	-	🟩	-	-	-
3	5.4 - Insider threat tactics	234		🟩	🟩	-	🟩	🟩	-	-	-	-	🟩	-	-	-	-	-	🟩	🟩	-	🟩	-	-	-	-	-	🟩	-	-
4	4.1.9 - Business email compromise (BEC)	133		🟩	🟩	🟩	🟩	🟩	-	-	-	-	-	-	-	-	-	-	🟩	-	-	-	-	-	-	🟩	-	-	-	-
5	5.5 - Information compromise or disclosure tacti	120		-	-	-	-	-	🟩	🟩	🟩	🟩	🟩	-	-	-	-	-	-	🟩	-	🟩	-	-	-	-	-	-	🟩	-
6	4.2.2 - Compromised credentials	120		-	-	-	-	-	-	-	🟩	🟩	🟩	-	-	-	-	-	🟩	🟩	-	-	-	-	🟩	-	-	-	-	-
7	4.2.4 - Compromised intellectual property (IP)	120		🟩	-	-	🟩	🟩	-	-	-	-	🟩	-	-	-	-	-	-	🟩	🟩	🟩	-	-	-	-	-	🟩	-	-
8	1.1.14 - Destructive malware	120		🟩	🟩	-	🟩	🟩	🟩	🟩	-	-	-	-	-	-	-	-	🟩	-	-	-	-	-	-	🟩	-	-	-	-
9	4.2.5 - Compromised network or system access	107		🟩	🟩	-	🟩	🟩	🟩	🟩	🟩	🟩	🟩	-	-	-	-	-	🟩	🟩	-	-	-	-	🟩	-	-	-	-	-
10	4.4 - Social engineering	107		🟩	🟩	🟩	-	-	-	-	-	-	-	-	-	-	-	-	🟩	-	-	-	-	-	-	-	🟩	-	-	-
11	1.1.3 - Remote access trojan (RAT) malware	107		🟩	🟩	-	🟩	🟩	🟩	🟩	-	-	-	-	-	-	-	-	🟩	-	-	-	-	-	-	🟩	-	-	-	-
12	1.1.7 - Botnet malware	93		🟩	🟩	-	🟩	🟩	🟩	🟩	-	-	-	-	-	-	-	-	🟩	-	-	-	-	-	-	🟩	-	-	-	-
13	5.2 - Post-attack tactics	80		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	🟩	-	🟩	-	-	-	-	-	🟩	-	-
14	4.1.14 - Payroll fraud scam	80		🟩	🟩	-	🟩	🟩	-	-	-	-	-	-	-	-	-	-	🟩	-	-	🟩	-	-	-	-	-	🟩	-	-
15	1.1.6 - Loader malware	80		🟩	🟩	-	🟩	🟩	🟩	🟩	-	-	-	-	-	-	-	-	🟩	-	-	-	-	-	-	🟩	-	-	-	-
16	5.2.12 - Impact tactic	67		🟩	🟩	-	-	🟩	🟩	-	-	-	-	-	-	-	-	-	-	🟩	🟩	🟩	-	-	-	-	-	-	🟩	-
17				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
18				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
19				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
20				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
				13	11	3	11	12	9	7	4	4	5	0	0	0	0	0	12	9	3	6	0	0	3	5	2	4	2	0
				Coverage emphasis															Deliverable emphasis											

If this is too simple for you or you need something more suitable for your needs, I suggest you head on over to ReqFast and have a look at their software, which contains stakeholder identification and tracking, requirements management and tracking, collection and vendor management, products and dissemination tracking, etc. etc. Their software comes preloaded with the entire content of the GIRH by Intel471, so if you outgrow their excel sheet, this is a good place to go to next.
https://reqfast.com/features/

Stakeholders	EXTERNAL				Primary Stakeholders						INTERNAL						
	Government Entities			Communities	Board / Business Leaders	CISO	Cyber Security/CDC		Fraud								
Deliverables	Authority	NCSC	xxx	X-ISAC			Cyber Security Manager	Team Members & Analysts	Fraud Manager	Team Members & Analysts							
Stakeholder Level	Strategic	Strategic	Strategic		Strategic	Strategic / Operational	Operational / Tactical	Tactical / Technical	Operational / Tactical	Tactical / Technical							
Products	x	x	x	x	x	Pri	Pri	x	Pri	x							
Reports	x	x	x	x	x	Pri	Pri	x	Pri	x							
Services					x	x	x	x	x	x							

Ledger:
Pri = the prioritized categories that will consume/use the data/info/intelligence
x = Might be useful to the stakeholder

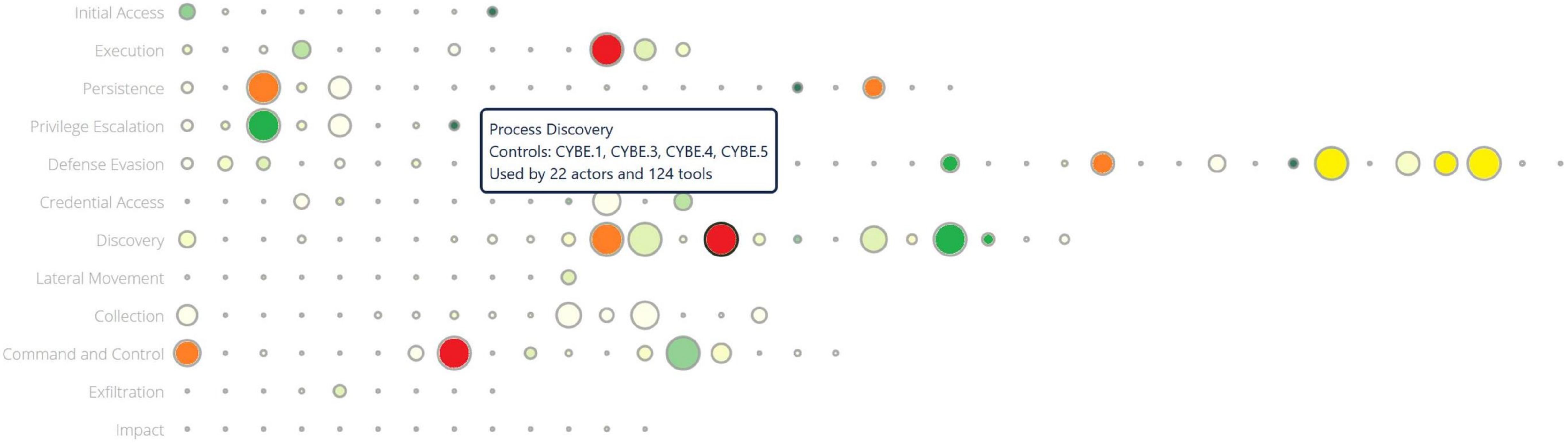
Intelligence Production Plan

Where does trust come from?

Deliver intelligence products that are V-TRACT

- Value
- Timely
- Relevant
- Accurate
- Consumable
- Tailored

Intelligence must provide value to those who “matter”



Process Discovery
Controls: CYBE.1, CYBE.3, CYBE.4, CYBE.5
Used by 22 actors and 124 tools

Mind Map

https://github.com/Errum/IntelArchitectureMap

Questions?

– To be or not to be