INTEL 471

Cyber Threat Intelligence: Maturity and Metrics

By Mark Arena, CEO
Intel 471
http://intel471.com

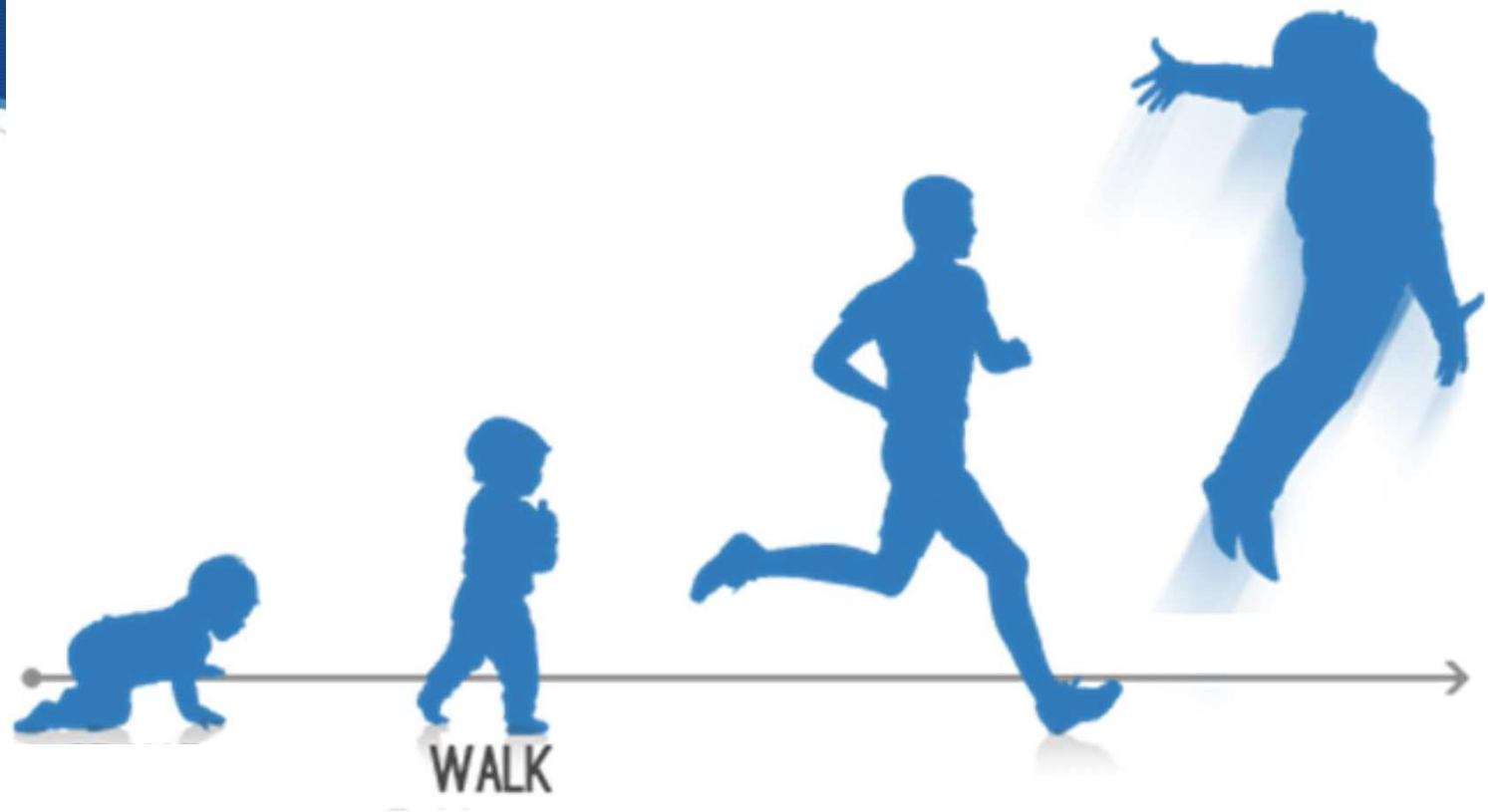
Intelligence definition

- "… intelligence is information that has been **analyzed** and **refined** so that it is **useful to policymakers in making decisions**—specifically, decisions about potential threats …"

  - https://www.fbi.gov/about-us/intelligence/defined


FLY
CRAWL
WALK
$RUN

I haz IOCs
Everything is targeted at me and unique to me! Cant Share!
IOCs or not actionable!
IP blocked!
Only able to consume tactical intelligence products



I haz IOCs with grouping and some context!
This is China APT - Ugly Panda!
I mostly copy content from vendor threat intel reports
Have some pre-determined requirements documented
It’s not relevant unless it hits us!

INTEL471

I have prioritized intelligence requirements
I produce unique, timely and relevant intelligence products to different internal consumers
I look at threats to my vertical/sector, not just my org
My intelligence program is expensive!

INTEL471

We see everything!
No one flies
We can jump a lot though

INTEL471

Cyber threat intelligence

- Two main customer/consumer intelligence product types:
  - Executives/decision makers
  - Network defenders
  - Others (i.e. fraud teams)
- Different intelligence products (deliverables) needed
- Current market focus?

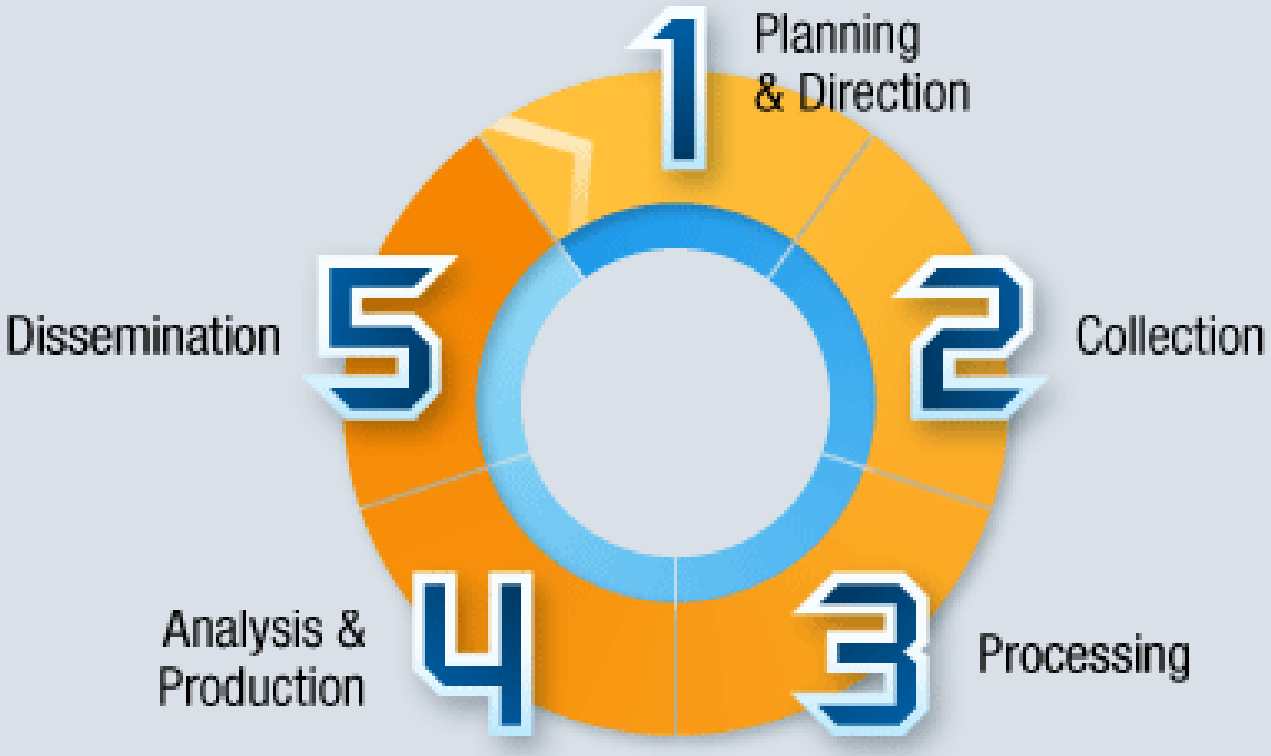
Relevance

- **Relevance**: does this intelligence (collection) satisfy one or more of my intelligence requirements

- If I don't have intelligence requirements (you should), does this impact me or my sector/vertical

Giving tactical intelligence products with IOCs to your C level

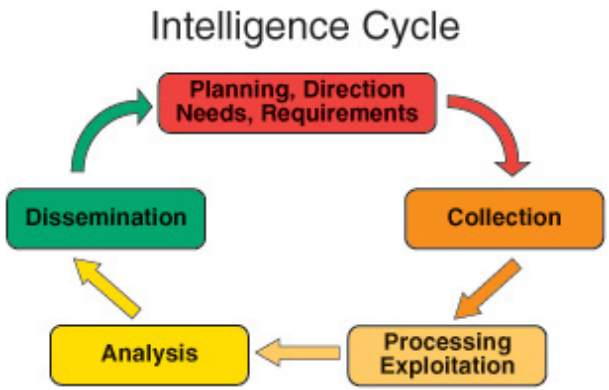
INTEL471


1
Planning
& Direction
2
Collection
3
Processing
4
Analysis &
Production
5
Dissemination

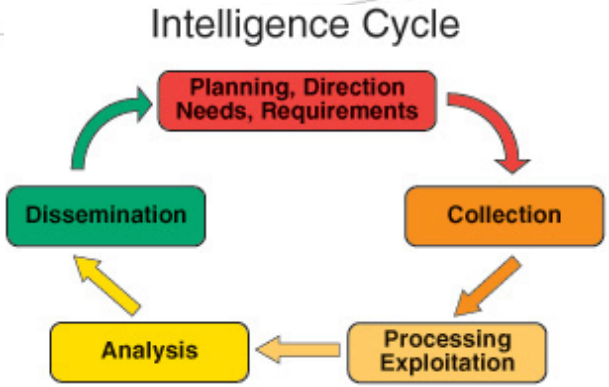
Your intelligence program's maturity is based on your ability to do each part of the intelligence cycle

Input into the intelligence cycle

Prioritized business risks



Output of the intelligence cycle



Decrease of probability or impact of a business risk occurring

Incident Centric Intelligence

Actor Centric Intelligence

Planning, Direction, Needs, Requirements

- Three requirements lists to build and maintain:
  - Production requirements – What will be delivered to the intelligence customer/consumer.
  - Intelligence requirements – What we need to collect to meet our production requirements.
  - Collection requirements – The observables/data inputs we need to answer our intelligence requirements.

Production requirements	Intelligence requirements
• What is needed to be delivered to the intelligence customer (the end consumer of the intelligence).	• What we need to collect to be able to meet our production requirements.

Production requirement	Intelligence requirements
What vulnerabilities are being exploited in the world that we can't defend against or detect?	- What vulnerabilities are currently being exploited in the wild? - What exploited vulnerabilities can my organization defend? - What exploited vulnerabilities can my organization detect? - What vulnerabilities are being researched by cyber threat actors?

Intelligence requirements	Collection requirements
• What we need to collect to be able to meet our production requirements.	• The observables/data inputs we need to answer the intelligence requirement.

Intelligence requirements	Collection requirements
What vulnerabilities are currently being exploited in the wild?	- Liaison with other organizations in the same market sector. - Liaison with other members of the information security industry. - Open source feeds of malicious URLs, exploit packs, etc mapped to vulnerability/vulnerabilities being exploited. - Online forum monitoring where exploitation of vulnerabilities are discussed/sold/etc.

Intelligence requirements	Collection requirements
What vulnerabilities are being researched by cyber threat actors?	- Online forum monitoring. - Social network monitoring. - Blog monitoring.

Requirements updates

- Update your requirements at least bi-annually
- Ad hoc requirements should be a subset of an existing requirement

Once you have your collection requirements

- Look at what is feasible.
  - Consider risk/cost/time of doing something in-house versus using an external provider
- Task out individual collection requirements internally or to external providers as **guidance**.
- Track internal team/capability and external provider ability to collect against the assigned guidance.

Collection

- Characteristics of intelligence collection:
  - Source of collection or characterization of source provided
  - Source reliability and information credibility assessed

- Some types of intelligence collection:
  - Open source intelligence (OSINT)
  - Human intelligence (HUMINT)
  - Liaison
  - Technical collection

NATO's admiralty system

- Used for evaluating intelligence collection

Reliability of Source	Accuracy of Data
A - Completely reliable B - Usually reliable C - Fairly reliable D - Not usually reliable E – Unreliable F - Reliability cannot be judged	1 - Confirmed by other sources 2 - Probably True 3 - Possibly True 4 – Doubtful 5 – Improbable 6 - Truth cannot be judged

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

Processing / Exploitation

- Is your intelligence collection easily consumable?
  - Standards
  - Centralized data/information (not 10 portals to use)
  - APIs
- Language issues?
- Threat intelligence platforms (TIPs) can help you here

Intelligence analysis

- Intelligence style guide
  - Defines format and meanings of specific terms within your intelligence products
- Analysts who are able to deal with incomplete information and predict what has likely occurred and what is likely to happen.
- Encourage analysts to suggest multiple hypothesizes.

Not analysis

- Dealing with facts only (intelligence analysts aren't newspaper reporters)
- Reporting on the past only, no predictive intelligence
- Copy and pasting intelligence reports from vendors
  - You have outsourced your intelligence function

Words of estimative probability

- Consistency in words used to estimate probability of things occurring or not occurring, i.e.

100% **Certainty**		
The General Area of Possibility		
93%	give or take about 6%	**Almost certain**
75%	give or take about 12%	**Probable**
50%	give or take about 10%	**Chances about even**
30%	give or take about 10%	**Probably not**
7%	give or take about 5%	**Almost certainly not**
0%	**Impossibility**	

Google search for: CIA words of estimative probability

Dissemination

- Intelligence products written with each piece of collection used graded and linked to source.
- Intelligence products sent to consumers based on topic and requirements met.
- What information gaps do we have?

Feedback loop

- We need to receive information from our intelligence customers on:
  - Timeliness
  - Relevance
  - What requirements were met?

- This will allow identification of intelligence (collection) sources that are supporting your requirements and which aren't

Intelligence program KPIs

- Quantity – How many intelligence reports produced?
- Quality – Feedback from intelligence consumers
  - Timeliness, relevance and requirements met

Item	Yes/ No
Regularly (bi-annually) updated requirements list that maps with your prioritized business risks.	
Ad hoc requirements meets existing documented intelligence requirements	
Documented production requirements	
Documented intelligence requirements	
Documented collection requirements	
Documented linking of collection requirements to internal teams/capabilities or external providers (guidance)	
Regular assessment of guidance versus output from internal capabilities and external providers (collection management)	

Item	Yes/ No
Intelligence collection is easily consumable, i.e. in a TIP	
Intelligence style guide	
Have an intelligence review and editing process	
Intelligence produced includes future predictions and doesn't just report on facts	
Sources used in intelligence products are linked and graded	
Knowledge gaps are identified in intelligence products and pushed back into the requirements part of the intelligence cycle	
Feedback is received from intelligence consumer/customer	

Item	Yes/ No
KPIs are generated for the intelligence program	
KPIs are generated for each part of the intelligence cycle including for internal and external sources of intelligence collection	
Have an intelligence (collection) management function that handles requirements to assigned guidance	

Questions