Cyber Threat Intelligence

What Are The Characteristics Of A Mature Cyber Threat Intelligence Program And How Is It Measured?

By Mark Arena

Mark Arena

- CEO of Intel 471
- Previously Chief Researcher at iSIGHT Partners (FireEye), Australian Federal Police

General infosec view on intelligence

When it comes to cyber threat intelligence, the security industry **mostly appears** to take the view that indicators of compromise (IOCs) are the best approach to initiate/drive the intelligence process.

CTI: An incident-centric approach

- Begins with detection of an event (reconnaissance or compromise)
- Any time we initiate/drive the intel process from indicators of compromise (IOCs)
- Enumerate TTPs and Actor (intent, goals, motivation) from IOCs

INTEL471

Pros of the incident-centric approach

- Direct relevance is established
- Potentially allows identification of the threat actors and groups that are targeting your organization
- Provides IOCs that can be used to aid in the identification of compromise from the same threat actor, campaign and incidents across an organization.

Cons of the incident-centric approach

- Reactive approach initiated after your organization has already been impacted to some degree.
- Focuses primarily on the attack surface and doesn’t reflect the process that the threat actor needs to go through to impact your organization.
- Difficult to be predictive.

The actor-centric approach to CTI

- The reverse of the incident-centric approach

Attribution - valuable or not?

- Lots of debate in the infosec community re: value of attribution (or not)

- I believe that attribution to various levels (person, group, nation-state, etc.) provides valuable insights that support decision-making at all levels

Which actors should I be interested in?

- Actors targeting my organisation
- Actors targeting other organisations in my sector/vertical
- Actors that are enablers for the actors targeting me and my sector
- All prioritised by business impact (intent will drive prioritisation)

With actors, we want to understand:

- Who are they?
- What are their associations with enabling actors and partners?
- What are their motivations?
- What are their technical skills and abilities?
- Who are they targeting?

Next step

- What are their TTPs?

- Fuse actor-centric information (through analysis) tied to TTPs and ideally campaigns and even IOCs

Pros of the actor-centric approach

- Enables your organization to be proactive and predictive.
- Provides context around an actor's motivations and their abilities before an incident occurs.
- Focused on adversary's business process rather than just the elements that (could) impact an organization's attack surface.

Cons of the actor-centric approach

- Relevance to your organization might not be readily apparent.
- It is challenging to gain and maintain accesses where threat actors and groups operate.
- Requires analytical effort to fuse with your other sources of information.
- Requires regularly updated prioritization of threat actors to focus on.
- May be missing IOCs to look for within your organization.

The formal definition of intelligence…

"… 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

Cyber threat intelligence

- Threat is a person with a motivation, goal and sophistication

- Malware isn’t a threat, the person using it is

INTEL471

Identify your intelligence customers

- Executive
- Corporate security
- Fraud
- Risk
- SOC

INTEL471

What intelligence products do they get?

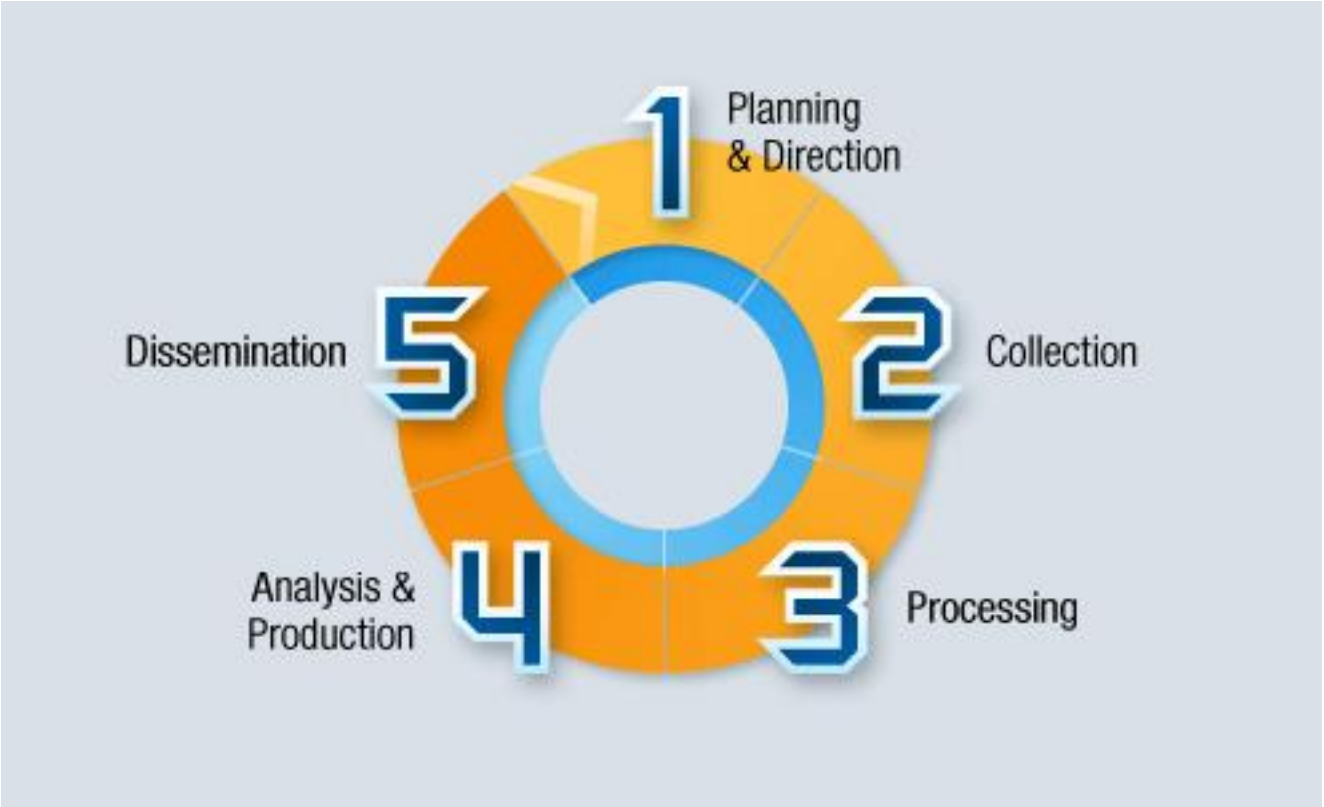
- Executive
- Corporate security
- Fraud
- Risk
- SOC

INTEL471

Giving a tactical intelligence product to an executive

INTEL471

Intelligence cycle



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

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
  - Changing threat landscape
  - Changing internal security posture
  - Changing business needs

- Ad hoc requirements should be a subset of an existing requirement
  - If it doesn’t fit, your original requirements are either not comprehensive enough or poorly written

Traceability

Enables the business justification of:

- Increased staff versus requirements asked of intel team
- Vendor purchases/subscriptions

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/outreach
  - 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

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

- Analysts who are able to deal with incomplete information and predict what has likely occurred and what is likely to happen

Intelligence analysis

- Intelligence style guide
  - Defines format and meanings of specific terms within your intelligence products

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**	

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

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

Putting it into practice with XYZ Online

- XYZ Online is a US headquartered company (approx. 5000 employees) that sells numerous goods online that ship to most places worldwide
- Has Chief Information Security Officer (CISO)
- Has 4 person cyber threat intelligence team

Excel spreadsheet example

Questions?

https://intel471.com/threatintelprogramchecklist.pdf

My blog on intelligence program strategy and tradecraft: https://medium.com/@markarenaau

INTEL471