Your Requirements are not My Requirements

Pasquale Stirparo
FIRST CTI Symposium 2019

$WHOAMI

- DFIR and CTI professional
  - Currently Security and Privacy Incident Manager @ Google
- Community
  - Founder/Organizer @BSidesZurich (https://bsideszh.ch/)
  - Mac4n6 Artifact Project, https://github.com/pstirparo/mac4n6
  - SANS Internet Storm Center, ENISA Threat Landscape SG
- Education
  - M.Sc. Computer Engineering, Polytechnic of Turin
  - Ph.D. Computer Security, KTH Stockholm
- Get in touch: @pstirparo

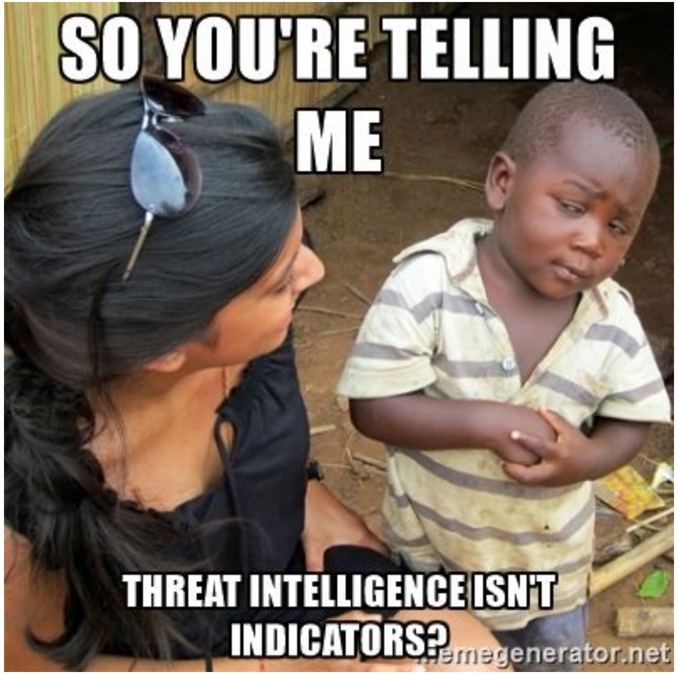
DISCLAIMER

The opinions expressed herein are my personal opinions and do not represent my employer’s view in any way.

What "Intelligence Requirements" are?

> *"Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence."[1]*

To go from information to intelligence, you need requirements



[1] http://www.thefreedictionary.com/intelligence+requirement

Why are so important?

- First step of Intelligence Cycle
  - Rings a bell?

- Information:
  - Quantity vs Relevancy
  - Prioritization

To be sure that the most relevant and most critical information is processed and not lost into the noise.

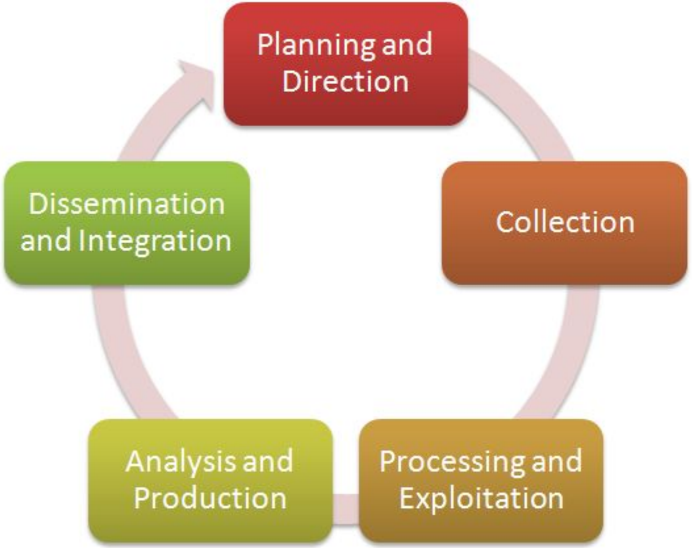


Image from countuponsecurity.com

Who Defines the Requirements?

Intelligence Requirements serve two purposes: Collection and Production

- Collection Requirements
  - Those are mostly defined by you, the CTI team
- Production Requirements
  - Usually come from “above”
  - RFI from Stakeholders / Management

High Level / Strategic Requirements

- Business industries of Operation
- Countries of Operation
- Business Top Critical Assets
- Potential adversaries: who would interested at your business?

Image from interismo.ch

Functional / Operational Requirements

- Physical external/perimetral exposure
- Physical internal exposure
- What type of attacks/threats do you fear the most?
- Who are your managed service providers?

Image from strategicbusinessdirect.com

Visibility / Technical Requirements

- Email Logs
  - timestamp, sender, recipient, subject, attachment(s) name, attachment(s) hash value, etc.
- Network
  - Proxy logs, Firewall logs, AD logs, etc.
  - Internal and third-party Passive DNS
- Endpoint visibility
  - What artifacts can you collect?
  - Memory dumps, registry hives, process executions, etc.

When Requirements meet Wish List

- External feeds and sources
  - Free/Paid feeds of indicators
  - Trusted private sharing communities
- Centralized Storage and Correlation
  - From spreadsheets to Threat Intelligence Platform (TIP)
  - Useful as central collection point of the collected intel.
  - Ideally integrated with other internal tools to allow automation
- People
  - Many different profiles/background is key
  - Fromer DFIR Ops, Reverse Engineers, Linguists, International Relations

RFI vs OMG

Someone high in the company heard a shocking news about a cyber cyber really cyber attack… is that true? Do you have intel on that? What about us?

- Be aware of the “jukebox effect”
- When done properly, those are legit requests
  - If you are tracking it, great
  - If you don’t, and consciously do so, write it down as well as the why
  - These requests may lead to new requirements

Some Examples: Corporate Espionage use case

Production Requirement
Your company is going to market with a new revolutionary product, the Board wants to make sure all sensitive IP (from design docs/blueprints to marketing campaigns, etc.) is not leaked or stolen.

Some Examples: Corporate Espionage use case

Collection Requirements

- Which attackers may be after this IP?
  - What is their Modus Operandi/TTP?
  - Do you have enough visibility to detect those?
  - Do you have access to (high) quality IoC from previous attacks?
  - OSINT monitoring for potential leaks?

- Where are those information stored and who has access to?
  - How are those systems protected/monitored?
  - People who can access are potential targets, looks for phishing/malicious emails?

- What about insider threat?

Some Examples: Vulnerabilities and Exploitation

Production Requirement
What are the vulnerabilities that are currently being exploited in the wild and that we should worry about? Are we protected against or can we detect them?

Some Examples: Vulnerabilities and Exploitation

Collection Requirements

- What vulnerabilities are currently being exploited?
  - Which of those may affect your organization?
  - Are any of those vulnerable system internet facing?
- Can you protect against them?
  - Is any patch available? Is it being prioritized?
- Can you detect attempts and/or successful exploitation?
  - What visibility/logs do you have?
  - What are you missing?

Conclusions

- Requirements are important, start from there
  - Will guide your **collection** and **prioritization**
  - Will help you find **gaps**

- Review them periodically
  - Threat landscape changes
  - You organization priorities may change as well

Conclusions

- Know and Talk to your Org
  - C-level, IT Infrastructure, etc.

- Best intel feed is from your own environment
  - Start with the analysis of past incidents
  - Do those incidents fit into the requirements that have been set?
  - If that incident will happen again, would you be able to either prevent or detect it? The requirements will tell you.

References

Clyde R. Heffter - CIA, *“A Fresh Look at Collection Requirements”*, https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol4no4/html/v04i4a03p_0001.htm

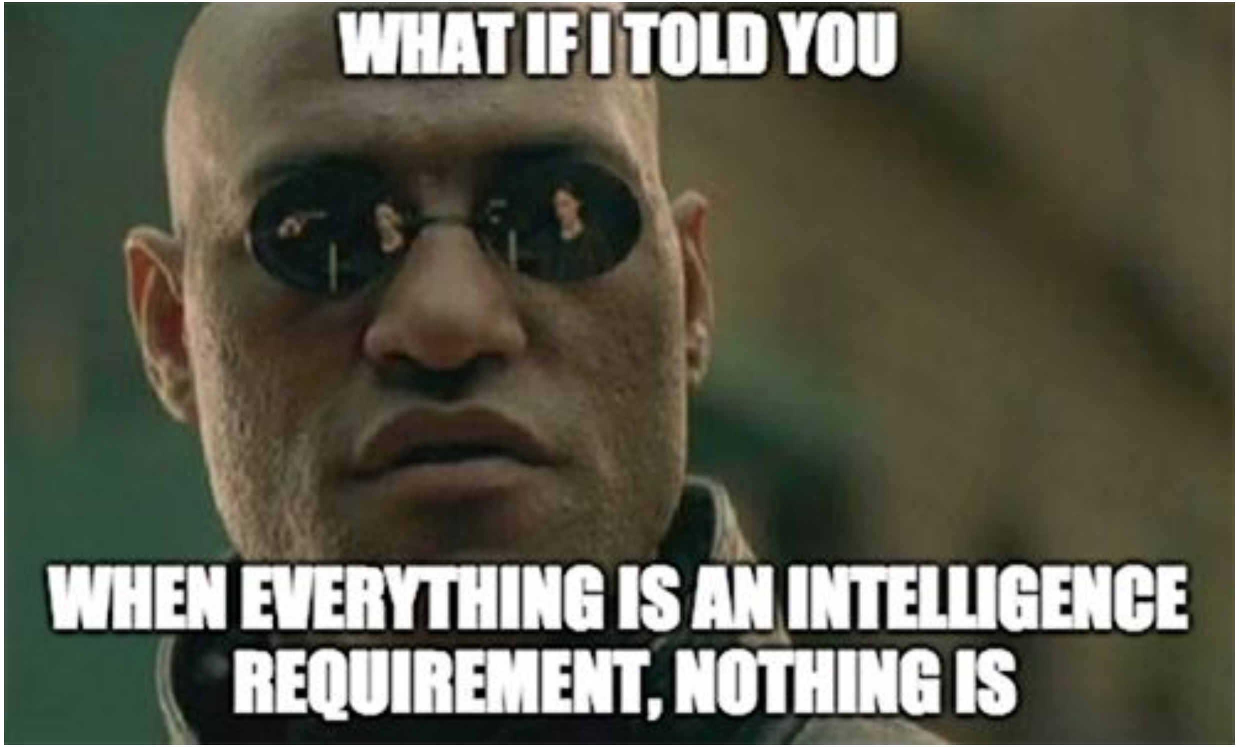
Pasquale Stirparo, *“Defining Threat Intelligence Requirements”*, https://isc.sans.edu/forums/diary/Defining+Threat+Intelligence+Requirements/21519/

Scott J. Roberts, *“CTI SquadGoals - Setting Requirements”*, https://medium.com/@sroberts/cti-squadgoals-setting-requirements-41bcb63db918

MWR Security, *“Threat Intelligence: Collecting, Analysing, Evaluating”*, https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/MWR_Threat_Intelligence_whitepaper-2015.pdf

Mark Arena, *“Cyber threat intelligence requirements: What are they, what are they for and how do they fit in the intelligence cycle?”*, https://www.linkedin.com/pulse/cyber-threat-intelligence-requirements-what-how-do-fit-mark-arena

Thank You!!!


WHAT IF I TOLD YOU
WHEN EVERYTHING IS AN INTELLIGENCE REQUIREMENT, NOTHING IS