

YOUR REQUIREMENTS ARE NOT  
MY REQUIREMENTS

**Pasquale Stirparo**  
**ENISA CTI 2020**

# \$WHOAMI

- DFIR and CTI professional
  - Security and Privacy Incident Manager @ Google
  - Research Associate @ Centre for Technology and Global Affairs @ Oxford University
- Community
  - Founder/Organizer [@BSidesZurich](https://bsideszh.ch/) (<https://bsideszh.ch/>)
  - Mac4n6 Artifact Project, <https://github.com/pstirparo/mac4n6>
  - 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.”<sup>1</sup>*

To go from information to intelligence, you need requirements



[1] DoD Joint Publication 2-0, [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2\\_0.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf)

# 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](http://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](https://www.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
  - Former 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
  - Your 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](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](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!!!

