ENISA NIS SUMMER SCHOOL 2019

CTI TRAINING

INTELLIGENCE REQUIREMENTS

(AKA HOW YOU CAN STOP TILTING AT WINDMILLS)

Image from heritage-history.com

Image from lapeceradepinocho.blogspot.com

Andreas Sfakianakis

CTI Professional

WHO AM I

FORTH Alumni
ENISA Trainee
ENISA NIS Summer School (x4)

- CTI and IR professional in Financial and Oil & Gas sectors
- External Expert for ENISA and European Commission
- Member of ENISA CTI Stakeholder Group
- Member of PC for FIRST CTI Symposium 2019 & 2020
- Get in touch: @asfakian / Website: www.threatintel.eu

tilting at windmills

References for this presentation: http://bit.ly/enisa_nis_2019

DISCLAIMER

- Original authors are referenced within the slide deck.

- References for this presentation: https://bit.ly/enisa_nis_2019

- Views are my own and not my employer's

AGENDA

- Setting the scene
- Intelligence requirements
- Examples
- Conclusions

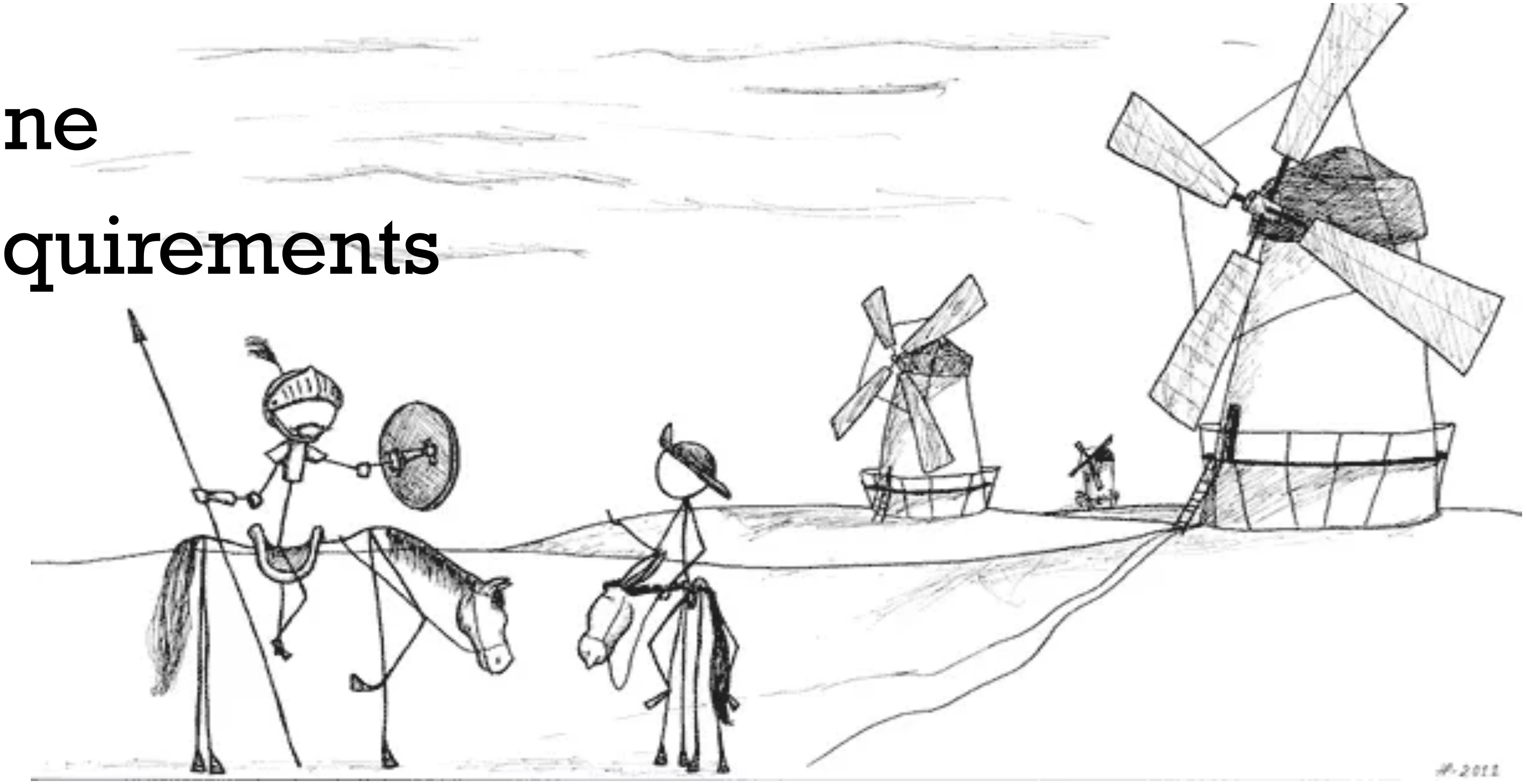


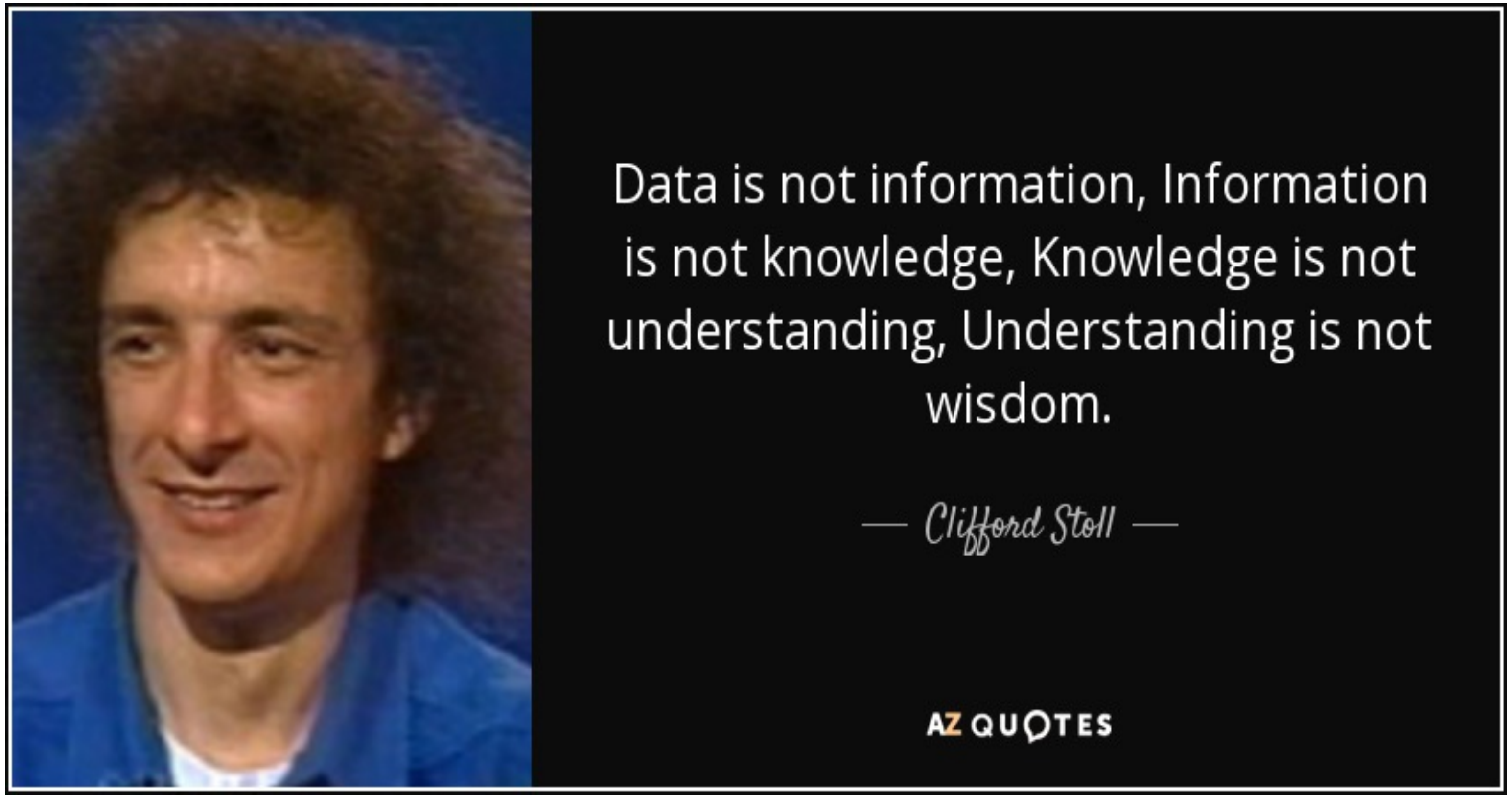
Image from hp-comic.com

Image from gatewaytotheclassics.com

SETTING THE SCENE: CTI STORIES

Language matters. Narrative matters. Framing matters.
People exist in and live by stories.
@treyka

WHEN EVERYTHING STARTED IN CTI!

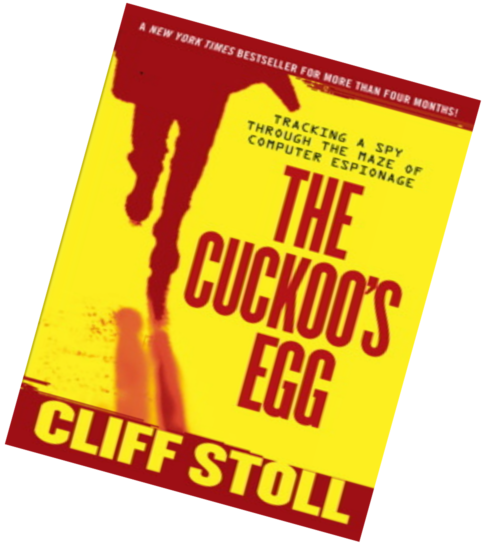


Data is not information, Information is not knowledge, Knowledge is not understanding, Understanding is not wisdom.

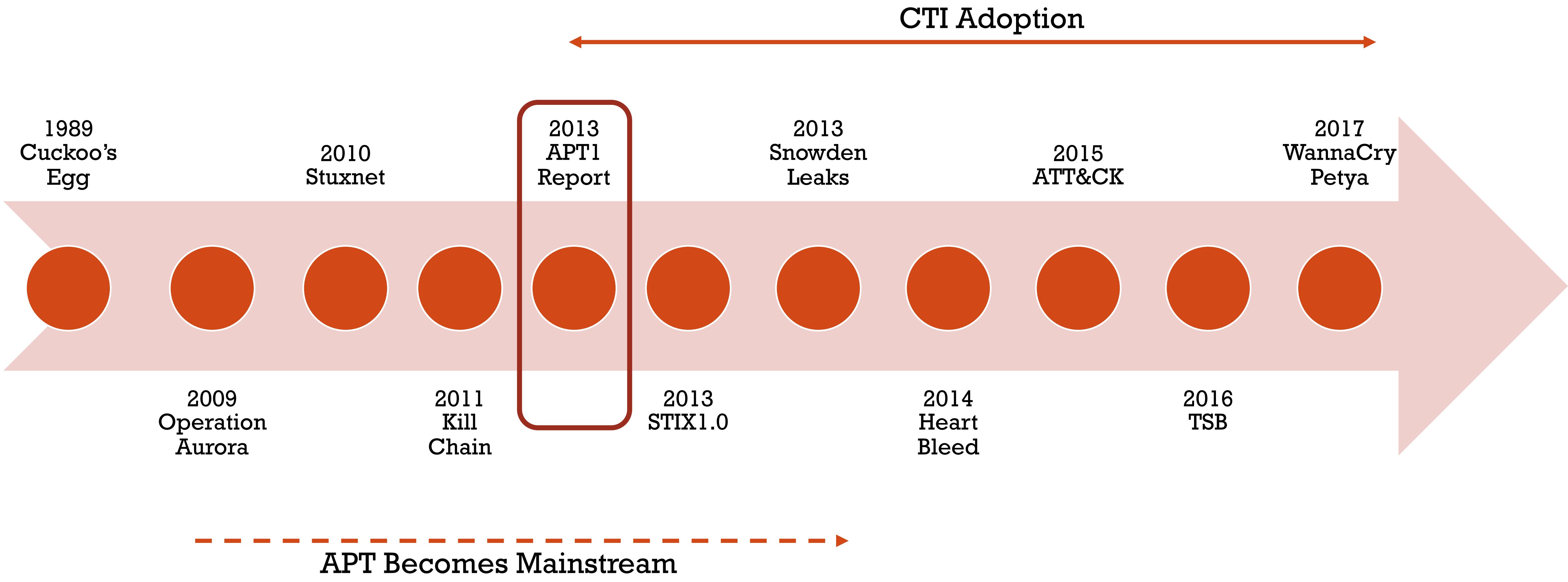
— Clifford Stoll —

AZ QUOTES

Image from azquotes.com


A NEW YORK TIMES BESTSELLER FOR MORE THAN FOUR MONTHS!
TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE
THE CUCKOO'S EGG
CLIFF STOLL

TIMELINE OF IMPORTANT EVENTS IN CTI



CTI Adoption

1989 Cuckoo's Egg

2009 Operation Aurora

2010 Stuxnet

2011 Kill Chain

2013 APT1 Report

2013 STIX1.0

2013 Snowden Leaks

2014 Heart Bleed

2015 ATT&CK

2016 TSB

2017 WannaCry Petya

APT Becomes Mainstream

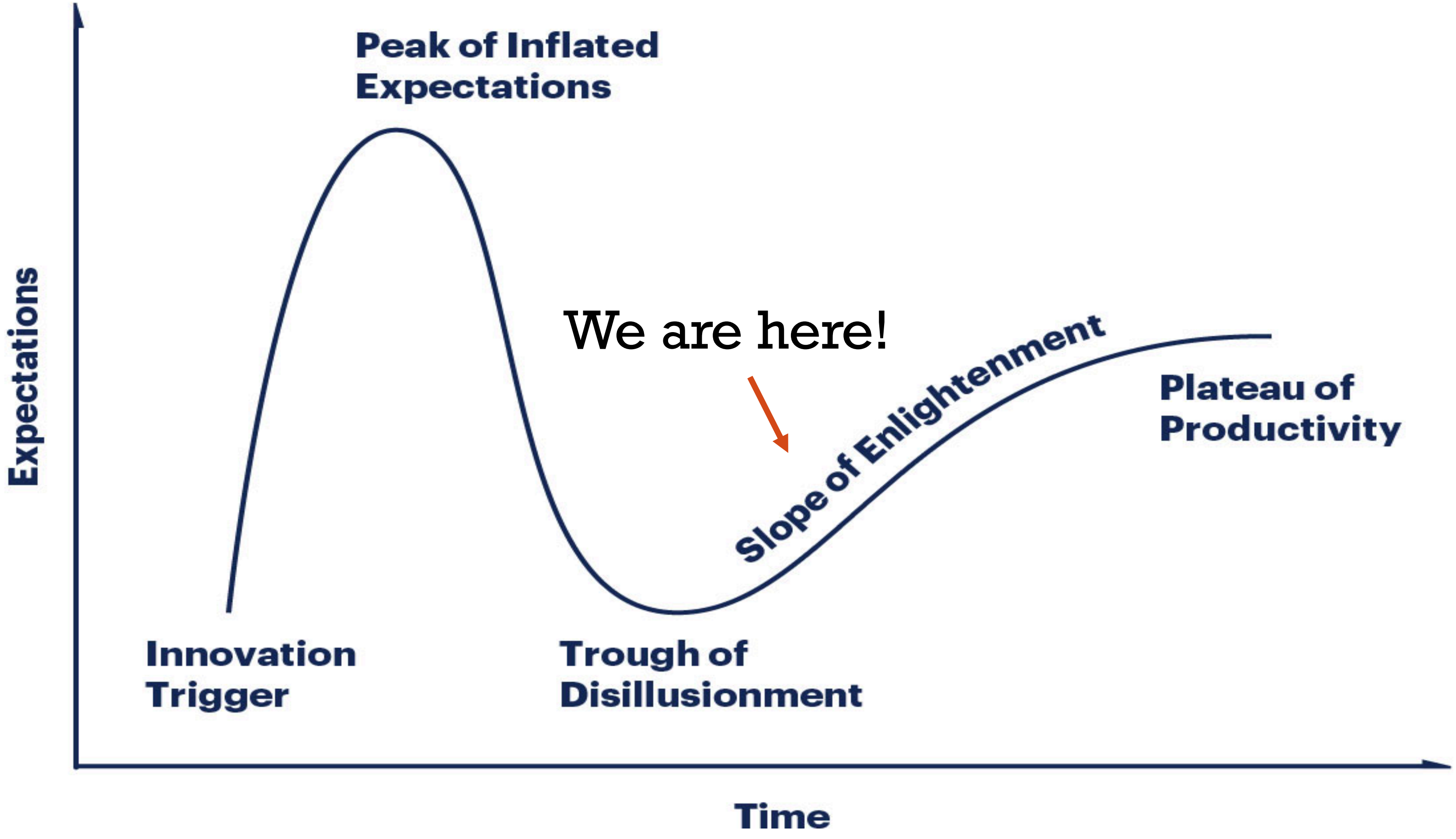
AS A COMMUNITY, WE DID GREAT PROGRESS!

	CYBER THREAT INTELLIGENCE	INCIDENT RESPONSE	SECURITY OPERATIONS
Adoption	Early adoption phase	Mainstream since ~2010	Mainstream since ~2005
Focus	External threat monitoring	Security incidents and risk escalation	Notable security event monitoring
Best practices	Evolving best practices	Mature best practices	Mature best practices
Technology enablement	Limited technology enablement	Mature technology enablement	Mature technology enablement

Reference:

eclectic iq

CTI HYPE CYCLE



Reference:

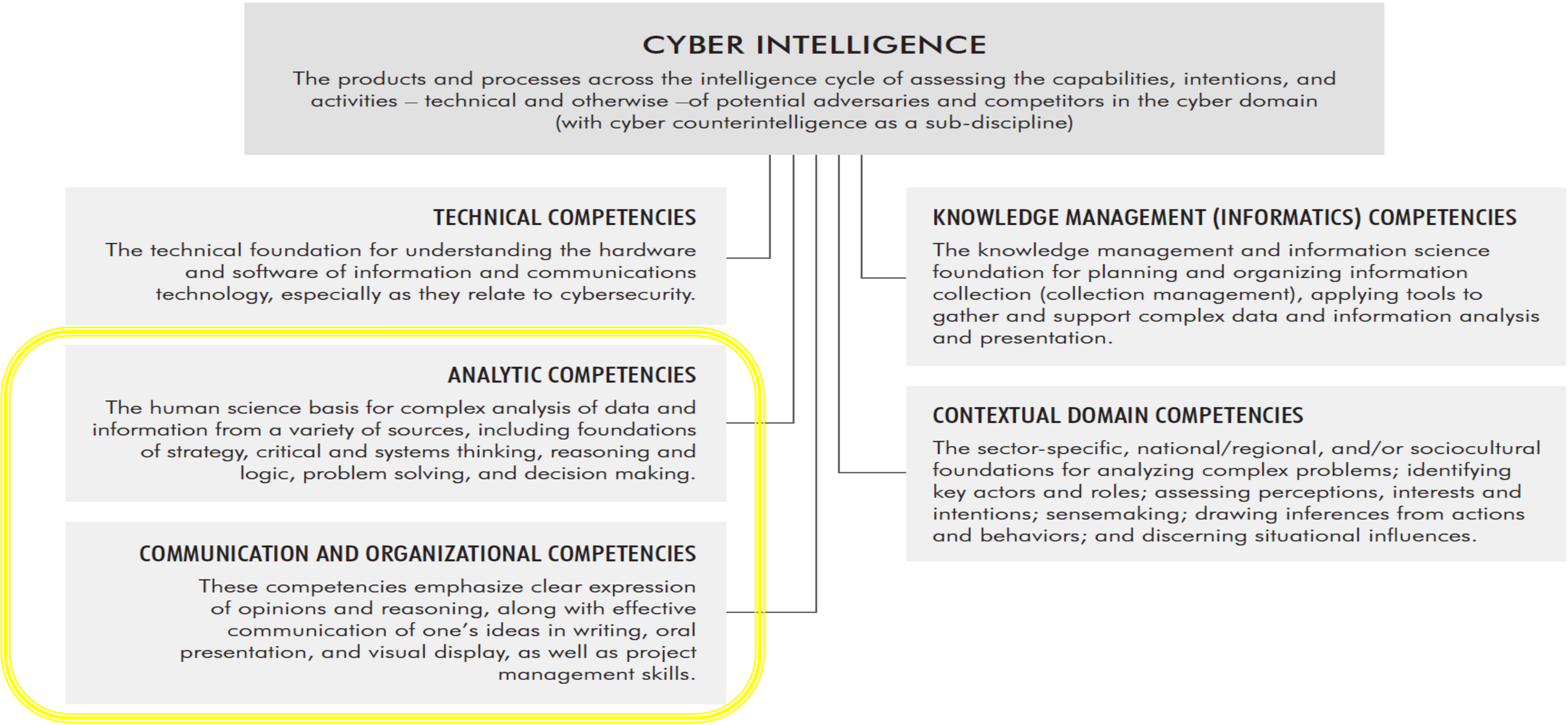
Gartner®

TODAY'S FOCUS

Image from imgbin.com

This will be a marvelous day for adventure, Sancho

THIS SESSION IS NOT TECHNICAL ☺



CYBER INTELLIGENCE

The products and processes across the intelligence cycle of assessing the capabilities, intentions, and activities – technical and otherwise –of potential adversaries and competitors in the cyber domain (with cyber counterintelligence as a sub-discipline)

TECHNICAL COMPETENCIES

The technical foundation for understanding the hardware and software of information and communications technology, especially as they relate to cybersecurity.

ANALYTIC COMPETENCIES

The human science basis for complex analysis of data and information from a variety of sources, including foundations of strategy, critical and systems thinking, reasoning and logic, problem solving, and decision making.

COMMUNICATION AND ORGANIZATIONAL COMPETENCIES

These competencies emphasize clear expression of opinions and reasoning, along with effective communication of one's ideas in writing, oral presentation, and visual display, as well as project management skills.

KNOWLEDGE MANAGEMENT (INFORMATICS) COMPETENCIES

The knowledge management and information science foundation for planning and organizing information collection (collection management), applying tools to gather and support complex data and information analysis and presentation.

CONTEXTUAL DOMAIN COMPETENCIES

The sector-specific, national/regional, and/or sociocultural foundations for analyzing complex problems; identifying key actors and roles; assessing perceptions, interests and intentions; sensemaking; drawing inferences from actions and behaviors; and discerning situational influences.

Reference:

INSA

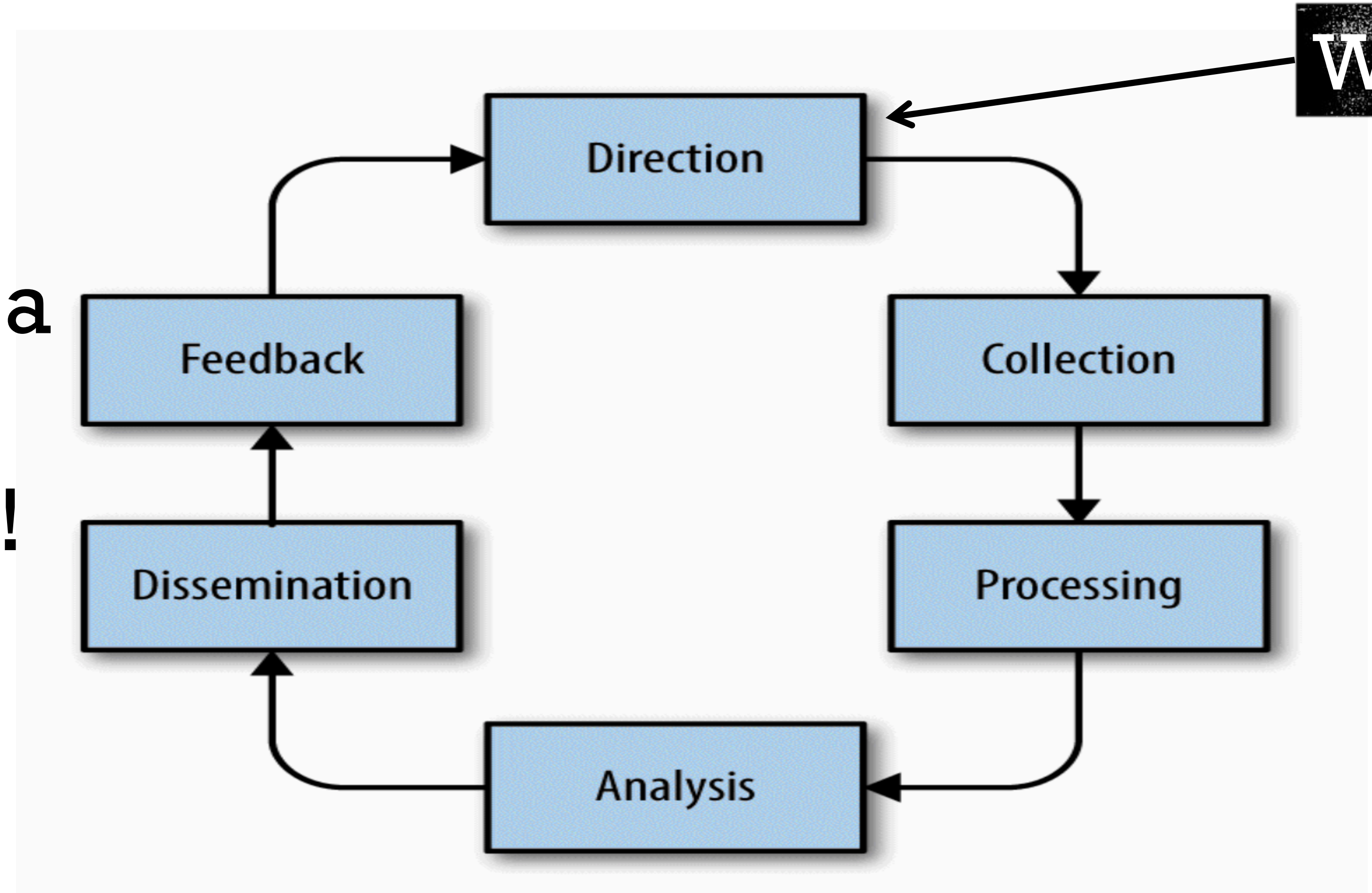
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

WELCOME TO THE WORLD OF INTELLIGENCE REQUIREMENTS

Image from wikimedia.org

THE INTELLIGENCE CYCLE!

Intelligence is a product
and a process!



We are here

INTELLIGENCE DIRECTION

- *How do CTI teams identify which threats are relevant to their organisations and how to prioritize them?*
- Have CTI teams identified and connected with their stakeholders?
- Have CTI teams captured the intelligence requirements of their stakeholders?
- How do CTI teams contribute towards the utmost goal of organisational risk reduction?
- "*CTI teams should not do intelligence for intelligence's sake, it costs money and time*" - Lauren Zabierek

CTI FOCUS AND STAKEHOLDERS

Tactical Intelligence

- Security Engineering
- SOC Team

Operational Intelligence

- Incident Responders
- Threat Hunters
- Vulnerability Management
- Red Team
- Fraud Team
- Sys Admins
- IT Managers

Strategic Intelligence

- C-Suite / Executives
- Group Security
- Risk Managers
- Business Stakeholders
- Regional Stakeholders
- IT Architects

WHAT INTELLIGENCE REQUIREMENTS ARE?

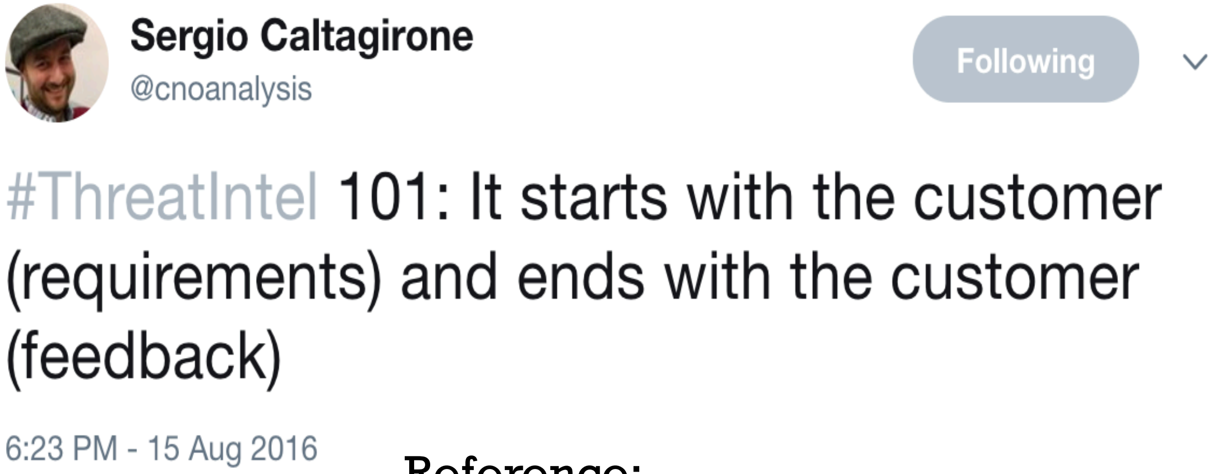
“Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence.”

DOD Joint Pub 2-0

https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf

INTELLIGENCE REQUIREMENTS 101

- Intelligence requirements are enduring questions that consumers of intelligence need answers to.
- Answer critical questions intelligence customers/stakeholders care about (not what YOU care about).



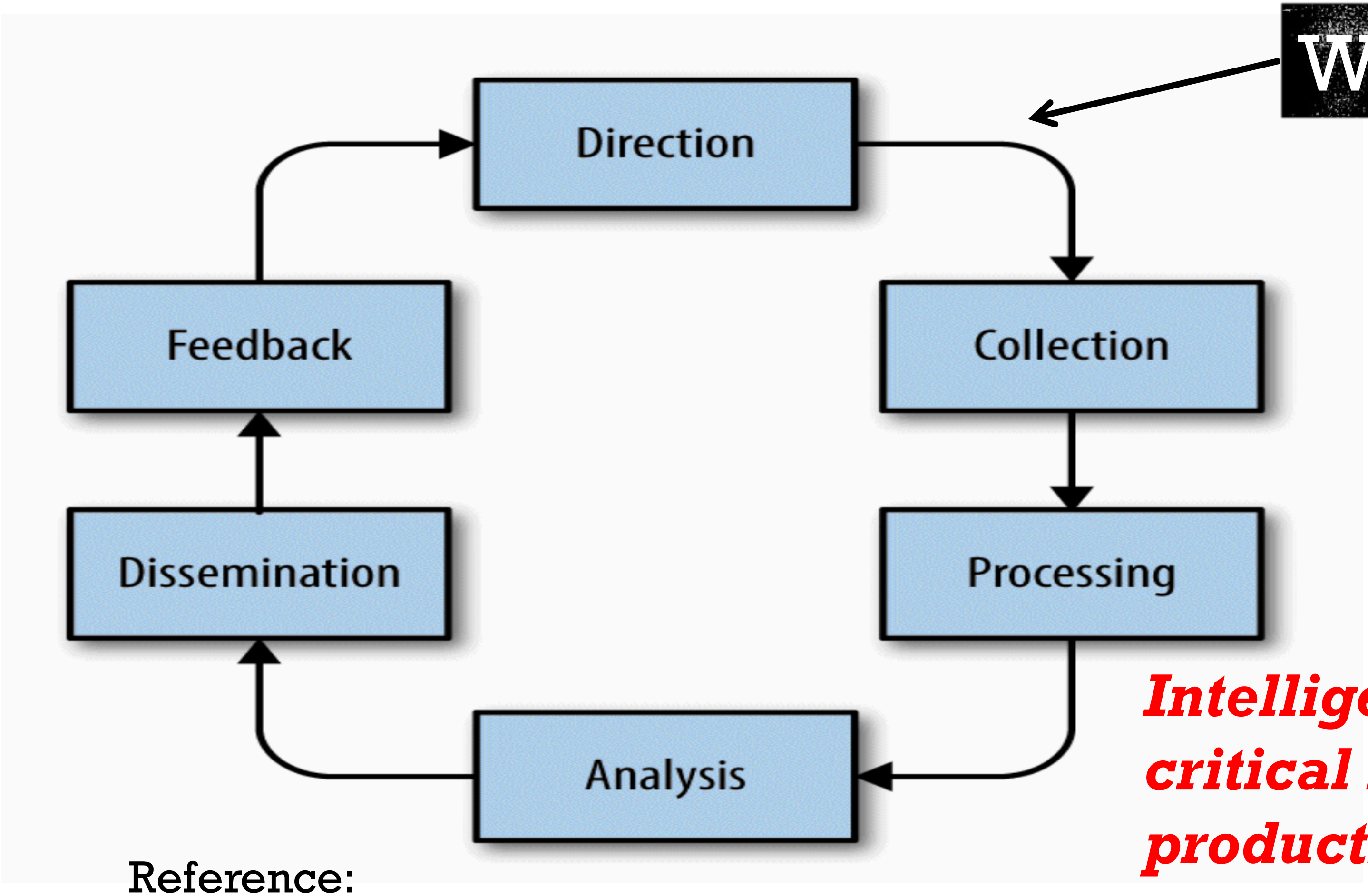
Sergio Caltagirone
@cnoanalysis

#ThreatIntel 101: It starts with the customer (requirements) and ends with the customer (feedback)

6:23 PM - 15 Aug 2016

Reference:
Sergio Caltagirone

REMEMBER THE INTELLIGENCE CYCLE!

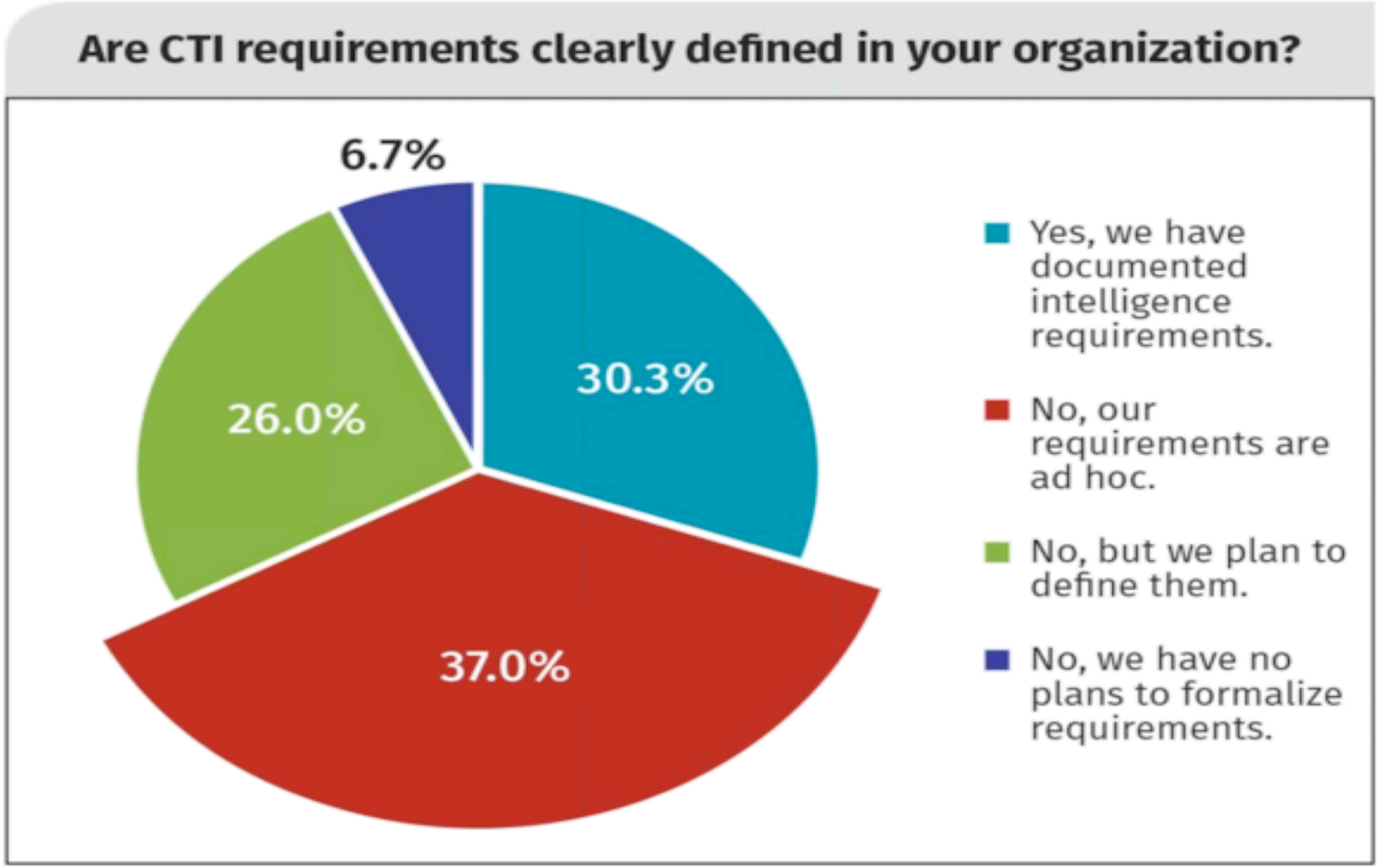


We are here

Intelligence requirements are really critical for intelligence collection and production phases!!

Reference:
Michael Rea

CLEARLY DEFINED INTELLIGENCE REQUIREMENTS?



Reference: SANS

PRIORITY INTELLIGENCE REQUIREMENTS (PIRS)

PIRs are the Intelligence requirements that the intelligence requirements that are seen as critical to accomplish mission.

If every requirement is critical then no requirement is critical

https://fas.org/irp/doddir/army/fm34-2/Appd.htm

WHERE TO START FROM?

- Past Incident Based Requirements
- Business Plan Based Requirements
- Geographic Based Requirements
- Technology Based Requirements
- Vertical Based Requirements

Reference:
Scott J Roberts

https://medium.com/@sroberts/cti-squadgoals-setting-requirements-41bcb63db918

INTELLIGENCE REQUIREMENTS CATEGORIES

- High Level / Strategic Requirements
- Functional / Operational Requirements
- Visibility / Technical Requirements

Reference:
Pasquale Stirparo

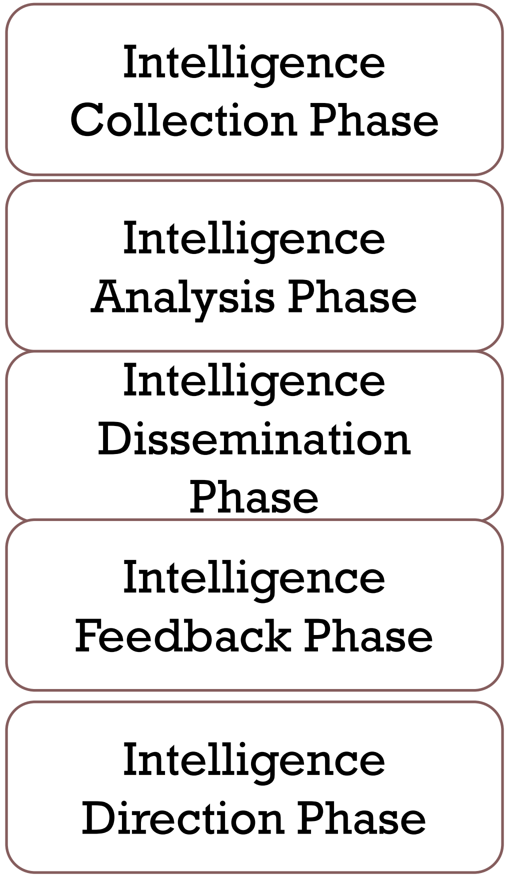
https://www.first.org/resources/papers/london2019/1430-1500-Your-Requirements-are-Not-My-Requirements-Speaker-Pasquale-Stirparo.pdf

GOOD PRACTICES: INTEL REQUIREMENTS

- Characteristics of intelligence requirements
- Update and communicate intelligence requirements
- Ad hoc requirements
- Documented and signed off

UTILIZING INTELLIGENCE REQUIREMENTS

- Intelligence collection driven by intelligence requirements
- Threat relevancy
- Shaping of the intelligence product(s)
- Business value and other metrics
- Traceability on resources and staffing



Intelligence Collection Phase

Intelligence Analysis Phase

Intelligence Dissemination Phase

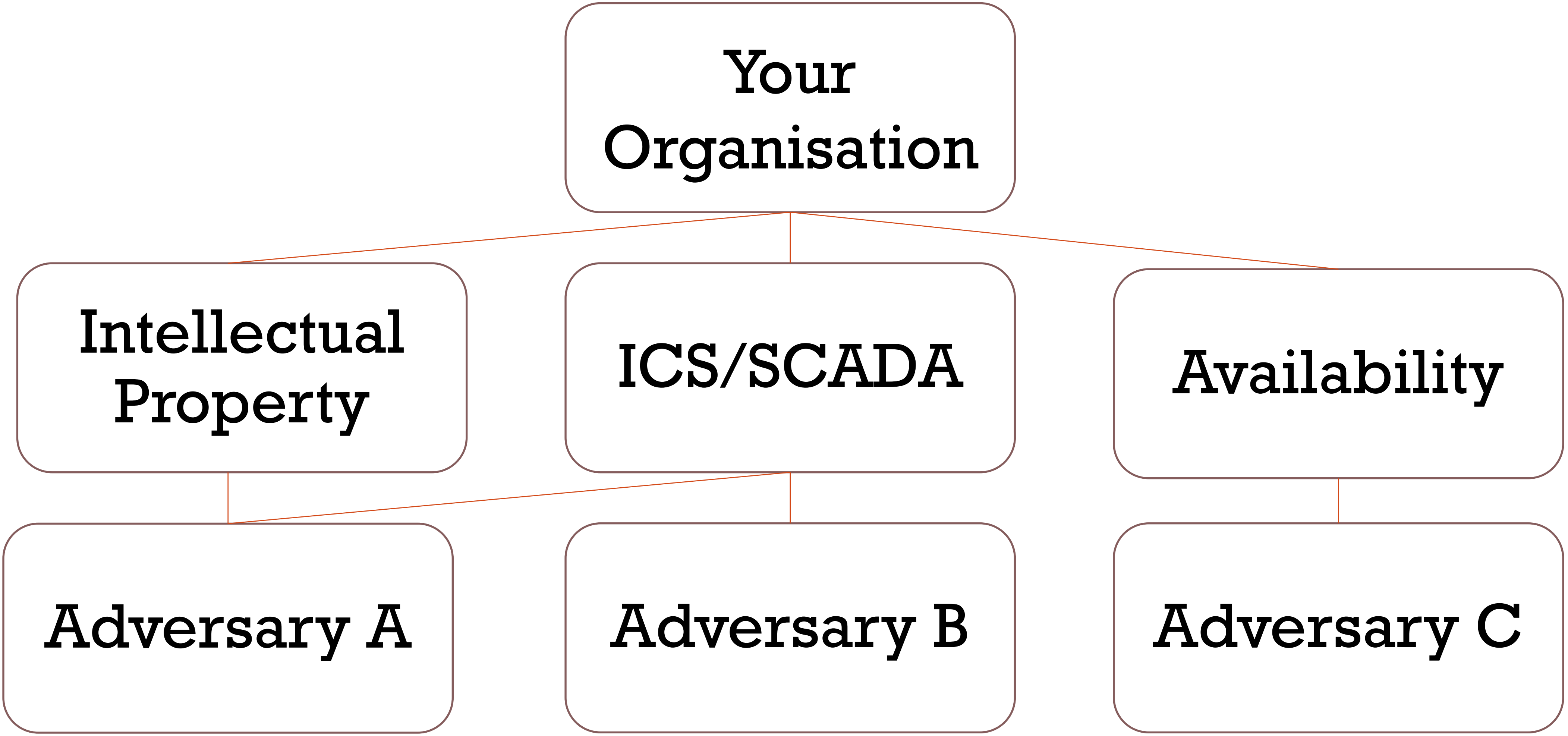
Intelligence Feedback Phase

Intelligence Direction Phase

A COUPLE OF TIPS AND LESSONS LEARNED

- Seek feedback
- Manage and educate your stakeholders
- Use the right terms
- Tell a story
- Build your organisation’s threat model

THREAT MODELING



Your Organisation

Intellectual Property

ICS/SCADA

Availability

Adversary A

Adversary B

Adversary C

Reference:
SANS

EXAMPLES

Image from gatewaytotheclassics.com

Image from blocs.xtec.cat

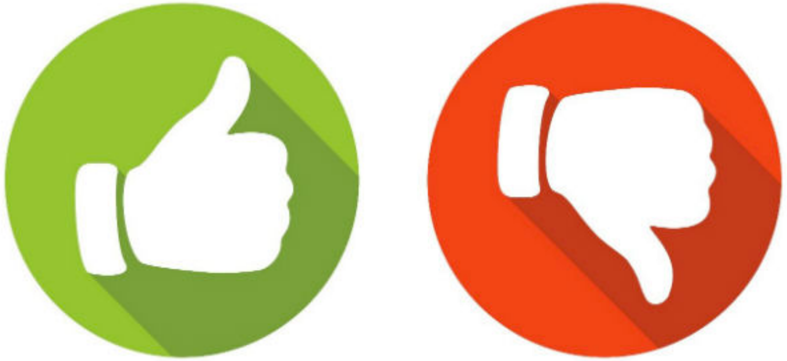
INTELLIGENCE REQUIREMENTS: REMEMBER!!!

- Decision centric: aids ONE decision.
- Singular: a strong requirement focuses on ONE question and only one question.
- Are specific: focuses on ONE activity/event/thing
- Timeliness: a requirement should capture the timeframe for usable intelligence.
- Are answerable using available assets and capabilities.

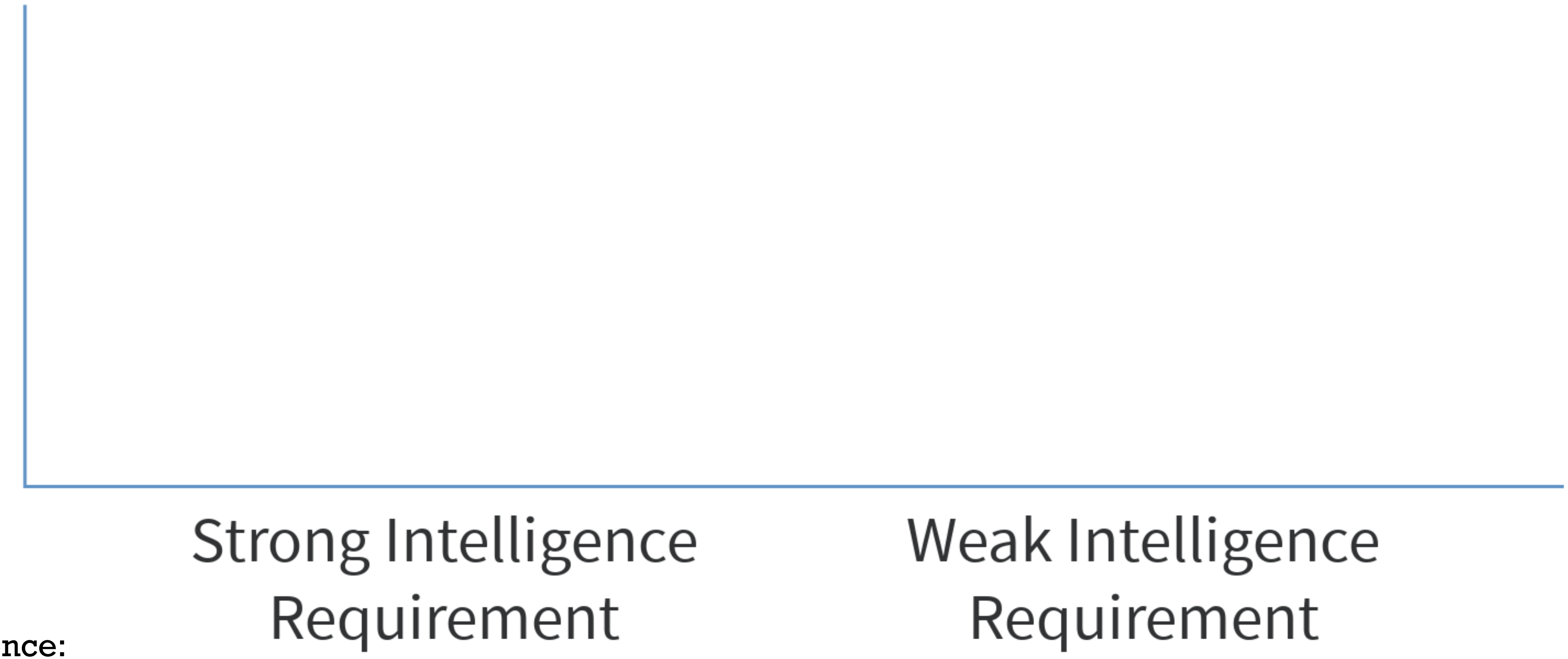
Reference:
Scott J Roberts

INTELLIGENCE REQUIREMENT EXAMPLE

- "Will the enemy attack? If so, where, when, and in what strength?"



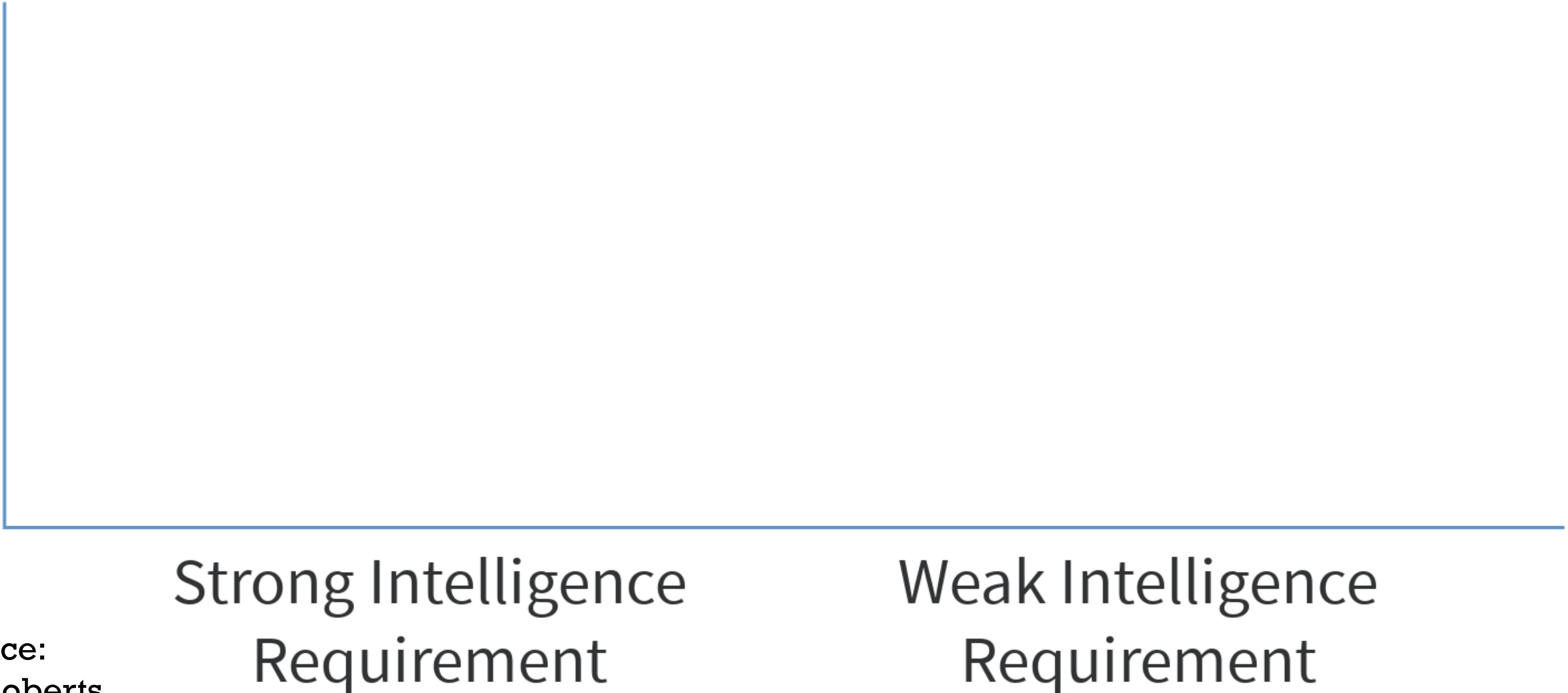
What adversaries might attack our company?



Reference:
Scott J Roberts

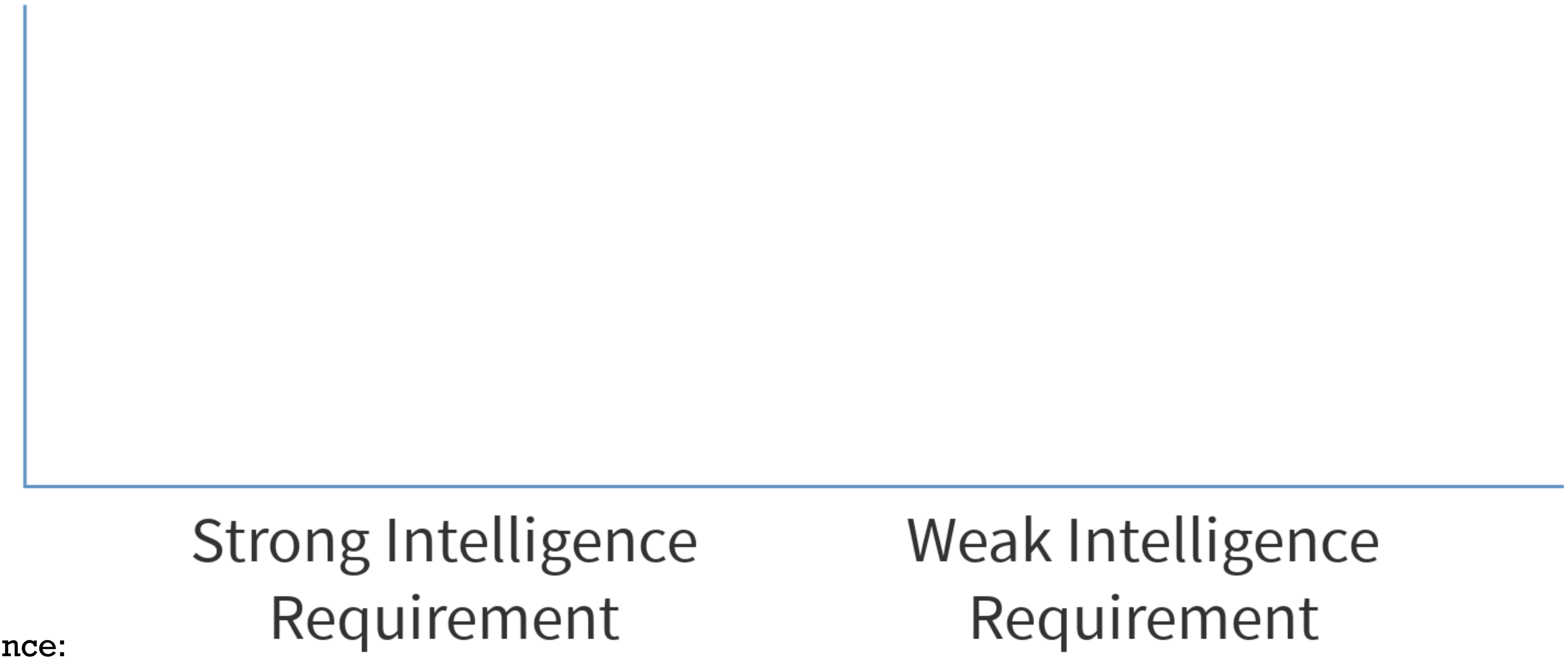
Total Results: 0

What indicators should we be using in our IDS?



Reference:
Scott J Roberts

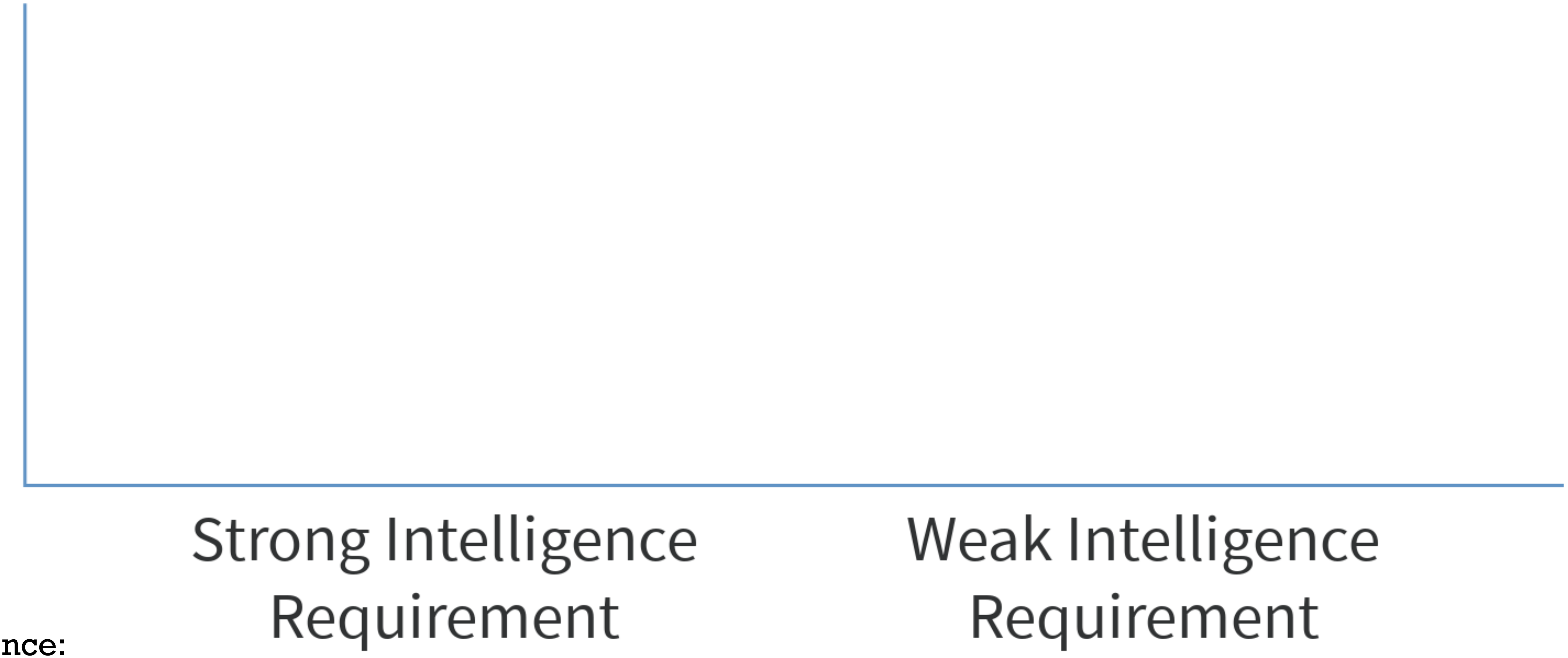
Is an adversary specifically targeting Region Y?



Total Results: 0

Reference:
Scott J Roberts

What malware should we look for on our network?

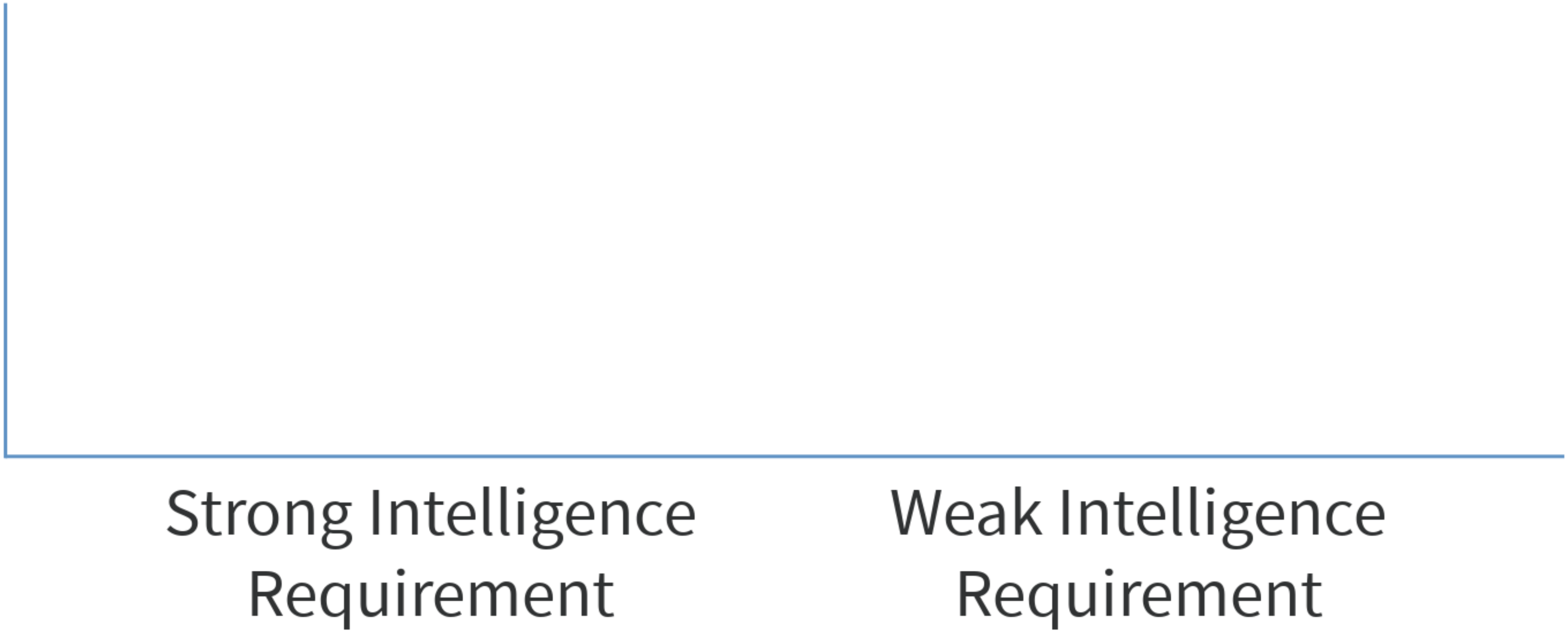


Reference:
Scott J Roberts

Total Results: 0

Start the presentation to see live content. Still no live content? Install the app or get help at **PollEv.com/app**

Is the level of cyber security investment matching our sector's threat landscape?



CORPORATE ESPIONAGE USE CASE

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

- What are our Intelligence Requirements?

Reference:
Pasquale Stirparo

https://www.first.org/resources/papers/london2019/1430-1500-Your-Requirements-are-Not-My-Requirements-Speaker-Pasquale-Stirparo.pdf

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?

- What are our Intelligence Requirements?

Reference:
Pasquale Stirparo

https://www.first.org/resources/papers/london2019/1430-1500-Your-Requirements-are-Not-My-Requirements-Speaker-Pasquale-Stirparo.pdf

Dulcinea

Dulcinea Watches as Don Quixote Wins Battles For Her

Image from elladocomicodedonquijote.wordpress.com

WRAPPING UP

FINAL REMARKS

- Identification of relevant stakeholders and get to know them
  - Connect with business and enterprise risk management cycles

- Better identification of your organisation’s operational environment
  - Get to know your organisation's crown jewels

- Capture, document and utilise your intelligence requirements

- Start the conversation

SITUATIONS WE WANT TO AVOID

https://grammarist.com/idiom/tilting-at-windmills/

https://en.wikipedia.org/wiki/Self-licking_ice_cream_cone

RESOURCES – INTELLIGENCE REQUIREMENTS

- US Military - Joint Publication 2-0
- SANS CTI Summit 2018 - I Can Haz Requirements? - Michael Rea
- CTI SquadGoals—Setting Requirements - Scott J Roberts
- SANS - Threat Intelligence: Planning and Direction - Brian Kime
- SANS - Defining Threat Intelligence Requirements – Pasquale Stirparo
- FIRST CTI 2019 - Your requirements are not my requirements – Pasquale Stirparo
- SANS CTI Summit 2018 - Intelligence Preparation of the Cyber Environment – Rob Dartnall
- Mark Arena - How to build a cyber threat intelligence program

SO, LET'S MAKE CTI GREAT (AGAIN)!

ENISA NIS Summer School 2019

Andreas Sfakianakis

CTI Professional

Sharing is caring!

References for this presentation: https://bit.ly/enisa_nis_2019