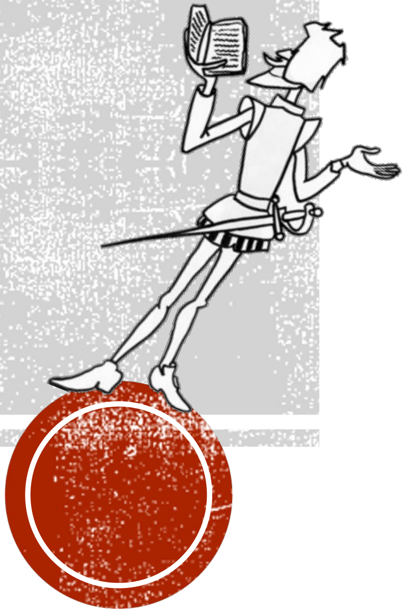
SPIN YOUR CTI PROCESS ROUND!



FIRST CTI Symposium 2023

8 November 2023

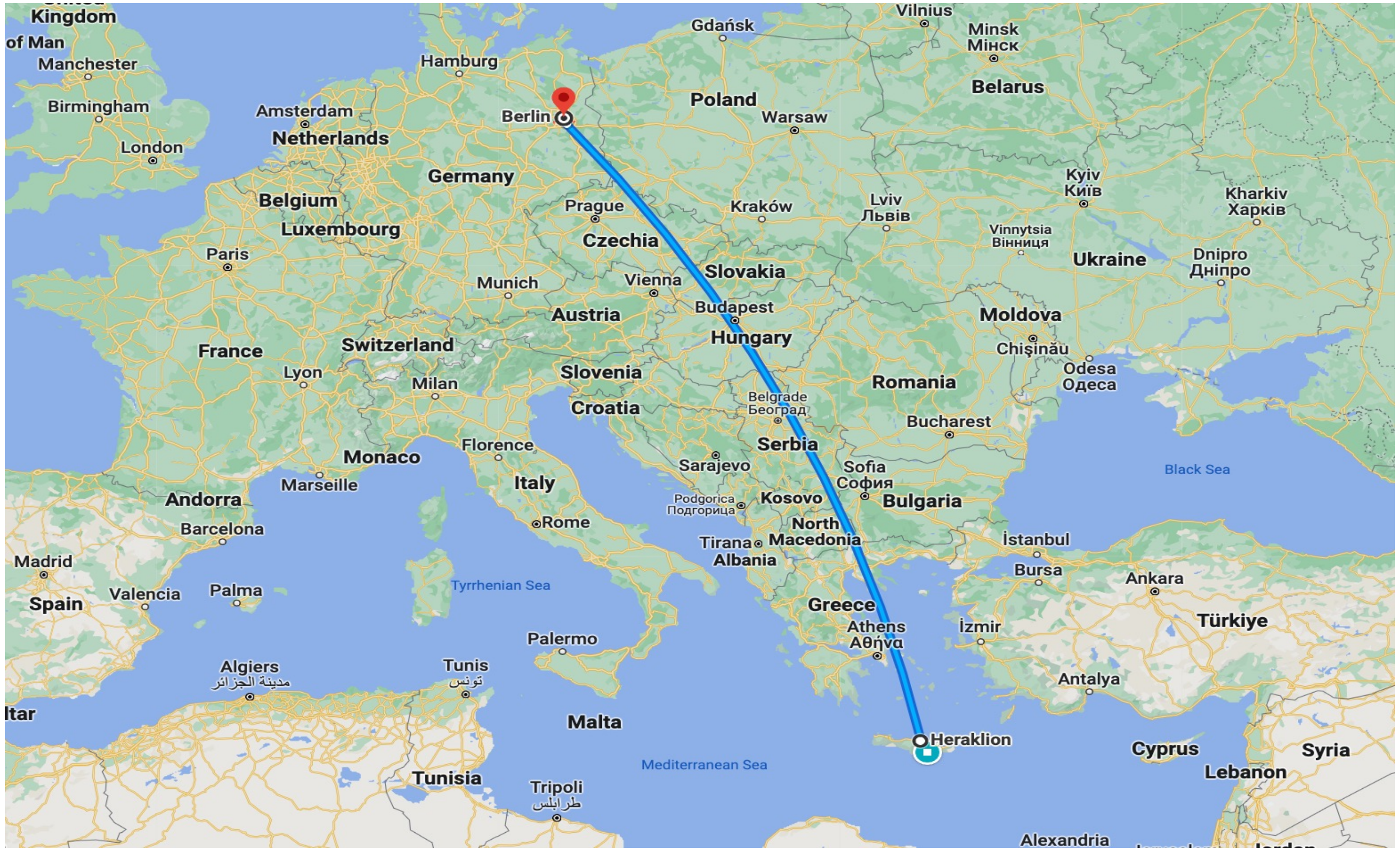
Andreas Sfakianakis

CTI Professional

TLP:CLEAR

THE BEST RUN SAP

CTI IS A JOURNEY!



#ctijourney

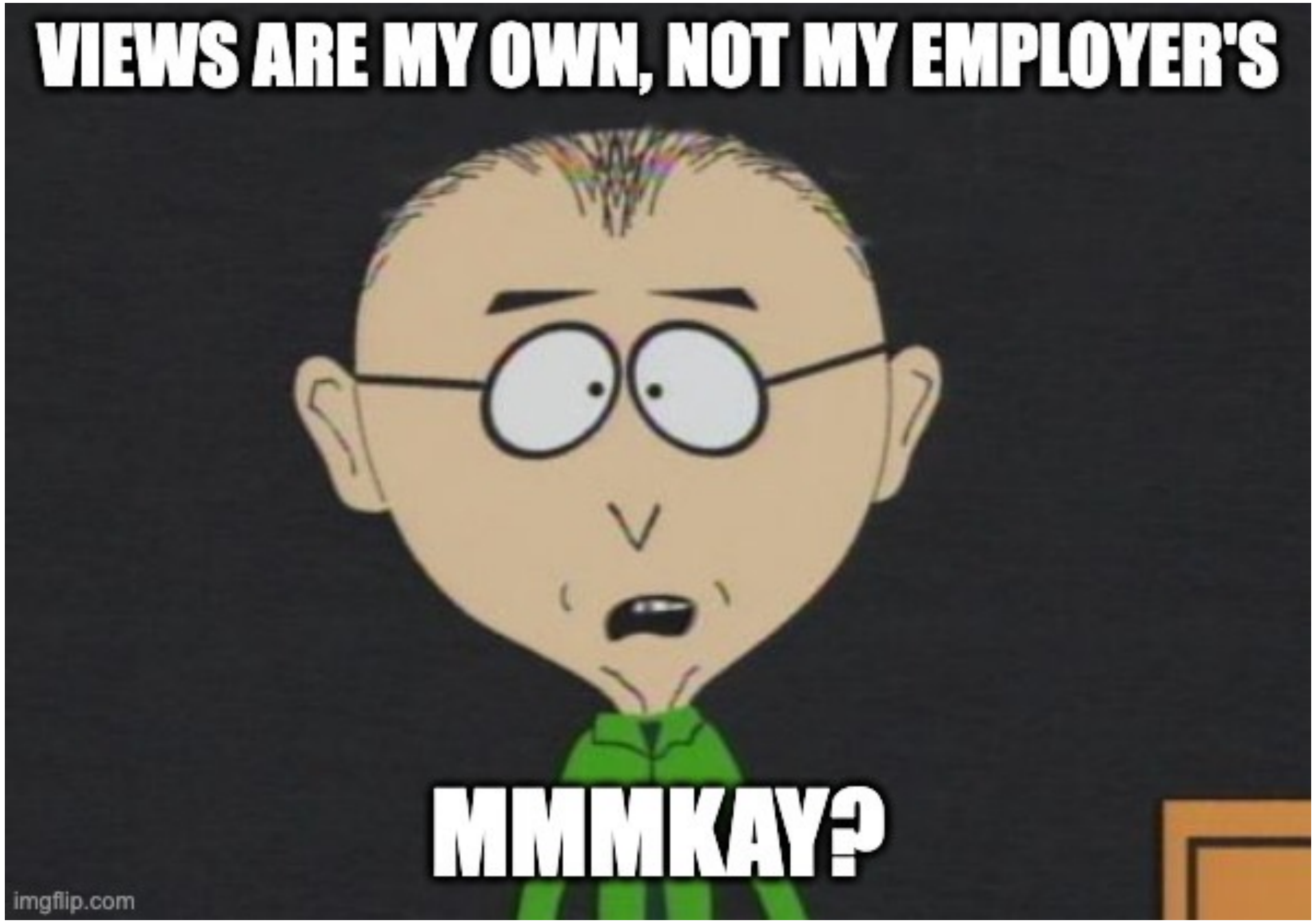
HOW CAN TEAMS EFFECTIVELY OPERATIONALIZE THEIR CTI PROCESS?

Problem Statement

WHO AM I

- CTI in Financial, Energy, and Technology sectors
- SANS, ENISA, FIRST.org, European Commission
- Twitter: @asfakian
  Mastodon: @asfakian@infosec.exchange
- Websites: www.threatintel.eu

DISCLAIMER



OUTLINE

Setting the scene

Workflow & Case Management

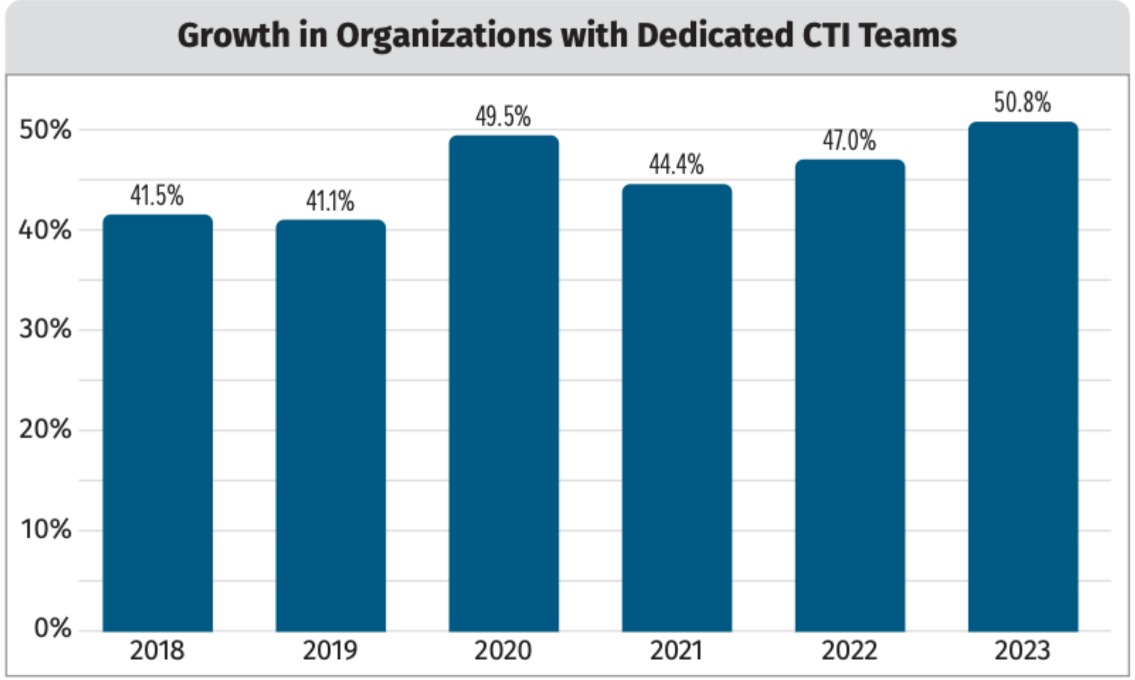
Basic Ingredients

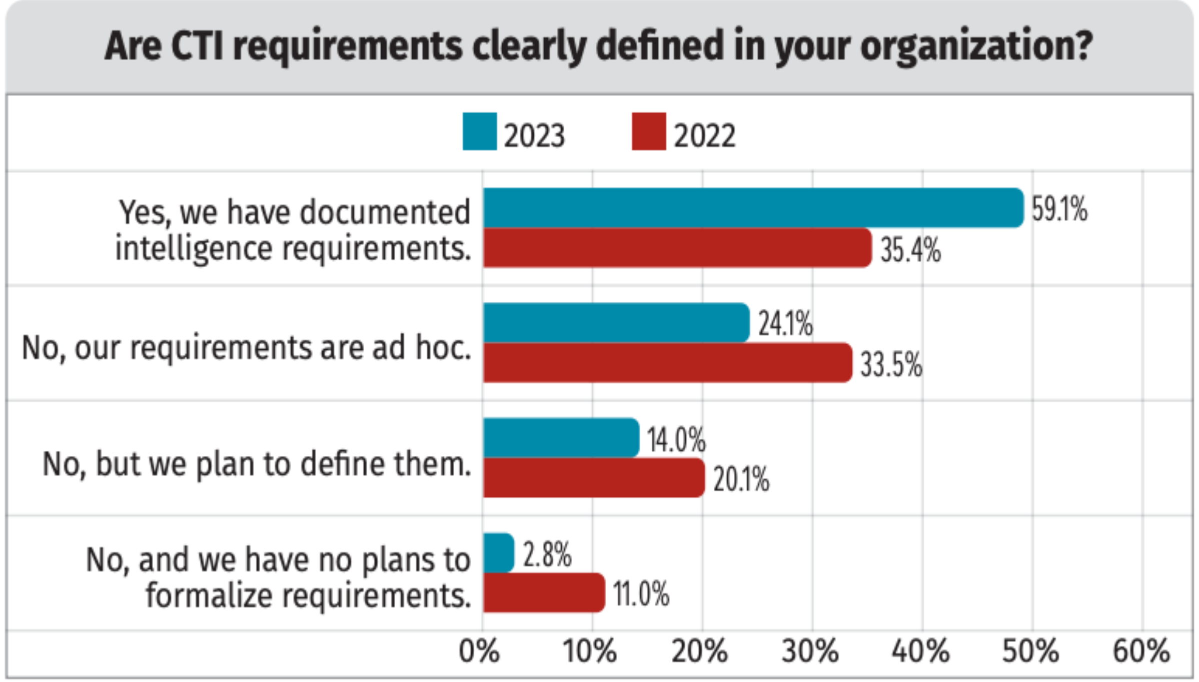
References used within this presentation: https://bit.ly/firstcti23

SETTING THE SCENE

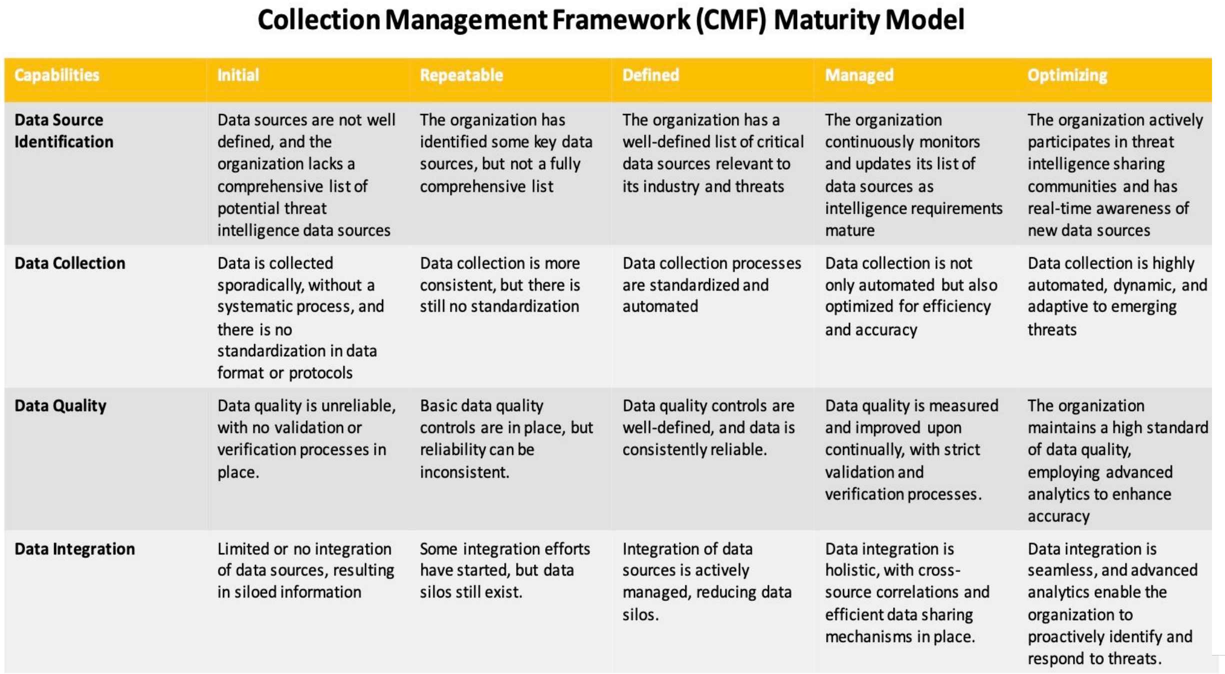
Image from gatewaytotheclassics.com

WE HAVE GONE A LONG WAY



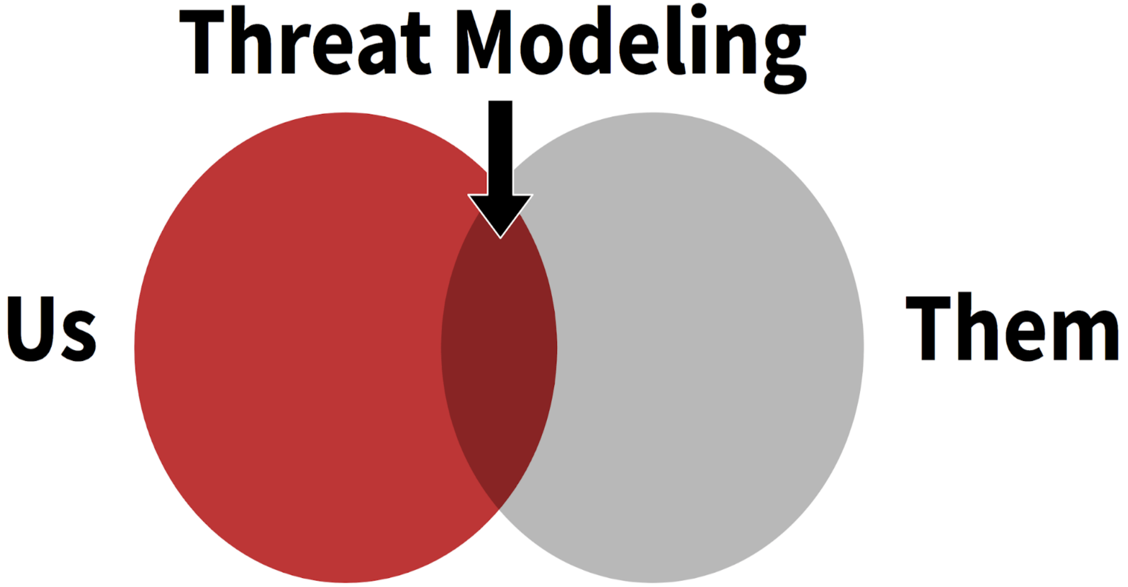


WE HAVE GONE A LONG WAY (2)



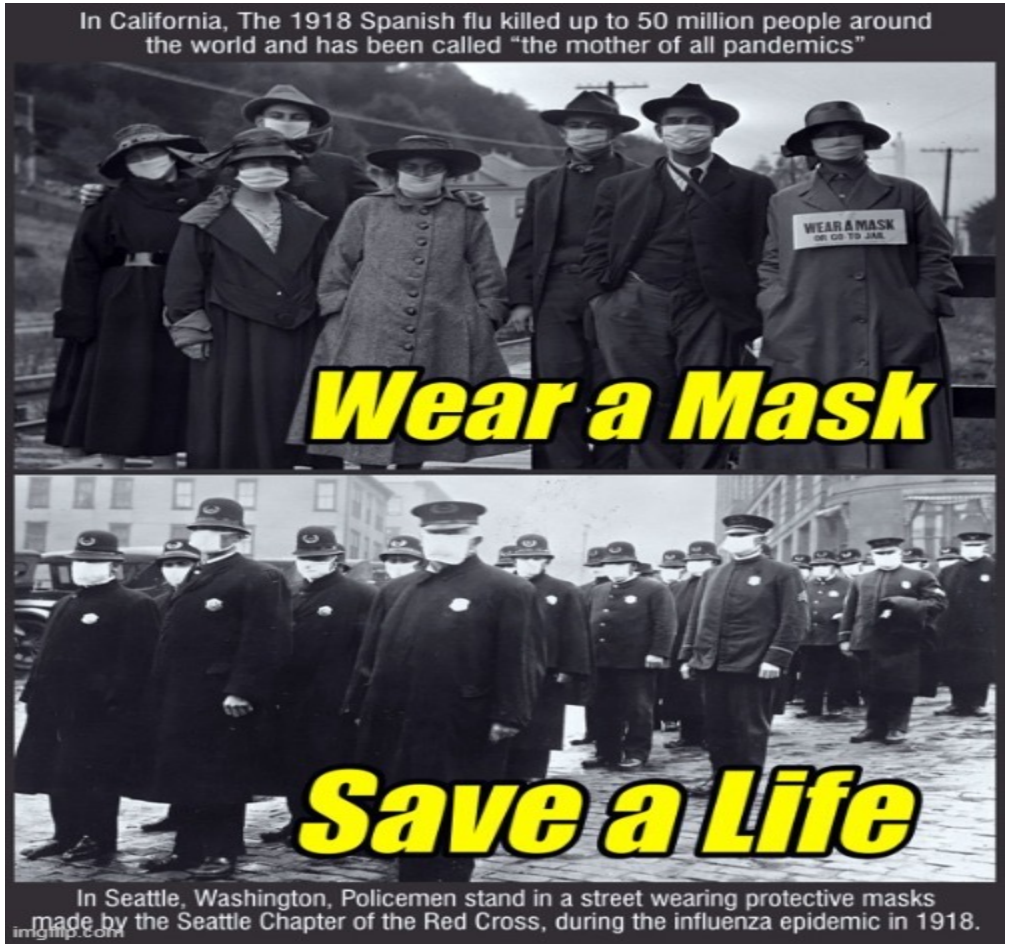
Collection Management Framework (CMF) Maturity Model

Capabilities	Initial	Repeatable	Defined	Managed	Optimizing
Data Source Identification	Data sources are not well defined, and the organization lacks a comprehensive list of potential threat intelligence data sources	The organization has identified some key data sources, but not a fully comprehensive list	The organization has a well-defined list of critical data sources relevant to its industry and threats	The organization continuously monitors and updates its list of data sources as intelligence requirements mature	The organization actively participates in threat intelligence sharing communities and has real-time awareness of new data sources
Data Collection	Data is collected sporadically, without a systematic process, and there is no standardization in data format or protocols	Data collection is more consistent, but there is still no standardization	Data collection processes are standardized and automated	Data collection is not only automated but also optimized for efficiency and accuracy	Data collection is highly automated, dynamic, and adaptive to emerging threats
Data Quality	Data quality is unreliable, with no validation or verification processes in place.	Basic data quality controls are in place, but reliability can be inconsistent.	Data quality controls are well-defined, and data is consistently reliable.	Data quality is measured and improved upon continually, with strict validation and verification processes.	The organization maintains a high standard of data quality, employing advanced analytics to enhance accuracy
Data Integration	Limited or no integration of data sources, resulting in siloed information	Some integration efforts have started, but data silos still exist.	Integration of data sources is actively managed, reducing data silos.	Data integration is holistic, with cross-source correlations and efficient data sharing mechanisms in place.	Data integration is seamless, and advanced analytics enable the organization to proactively identify and respond to threats.



Brian Warehime

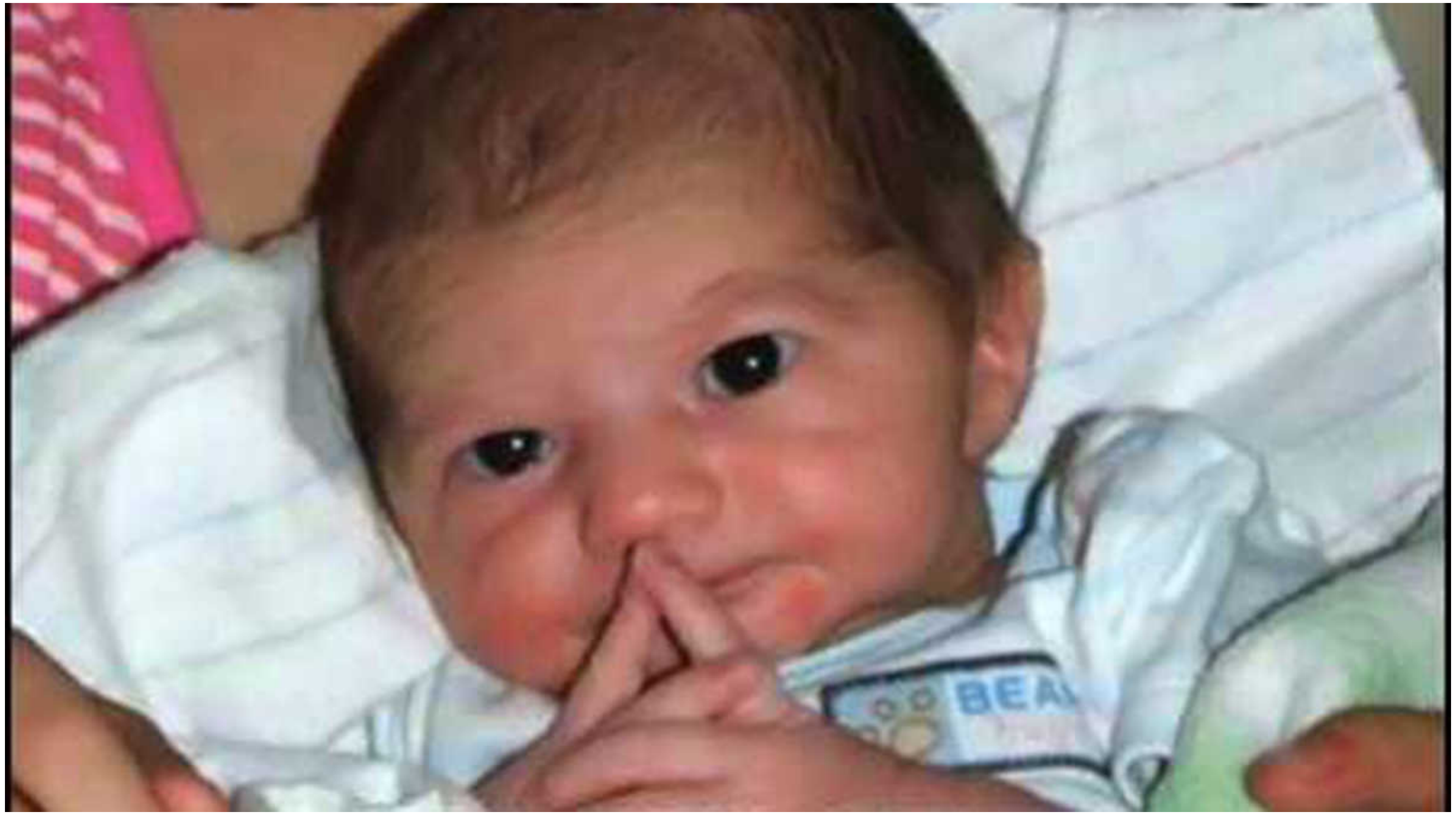
WHAT'S OLD IS NEW AGAIN



In California, The 1918 Spanish flu killed up to 50 million people around the world and has been called "the mother of all pandemics"

In Seattle, Washington, Policemen stand in a street wearing protective masks made by the Seattle Chapter of the Red Cross, during the influenza epidemic in 1918.

WHERE DO WE GO FROM HERE?



WORKFLOW & CASE MANAGEMENT

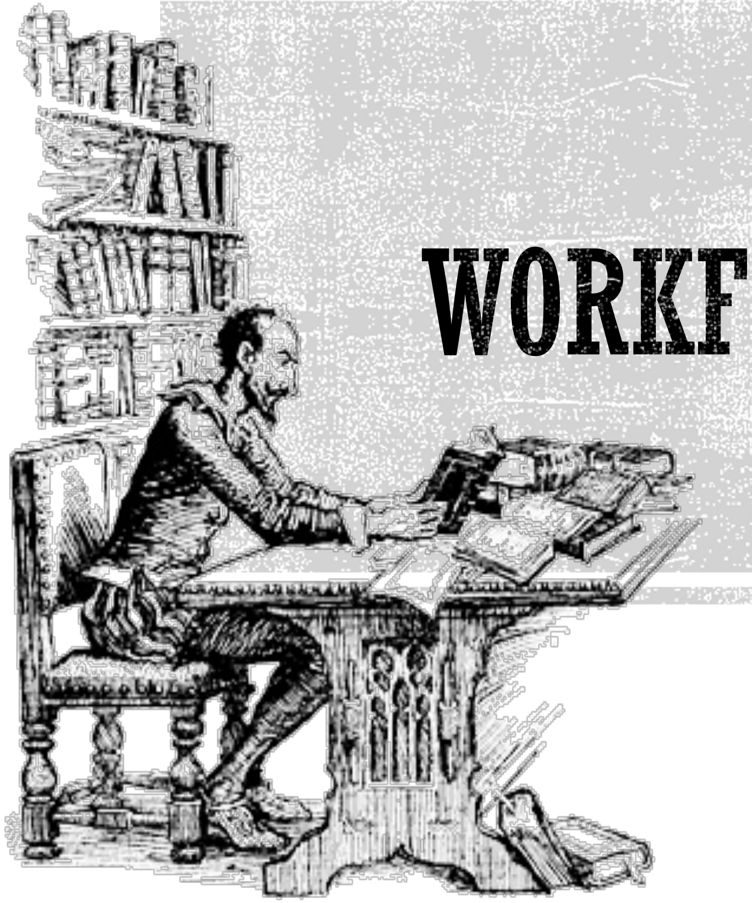
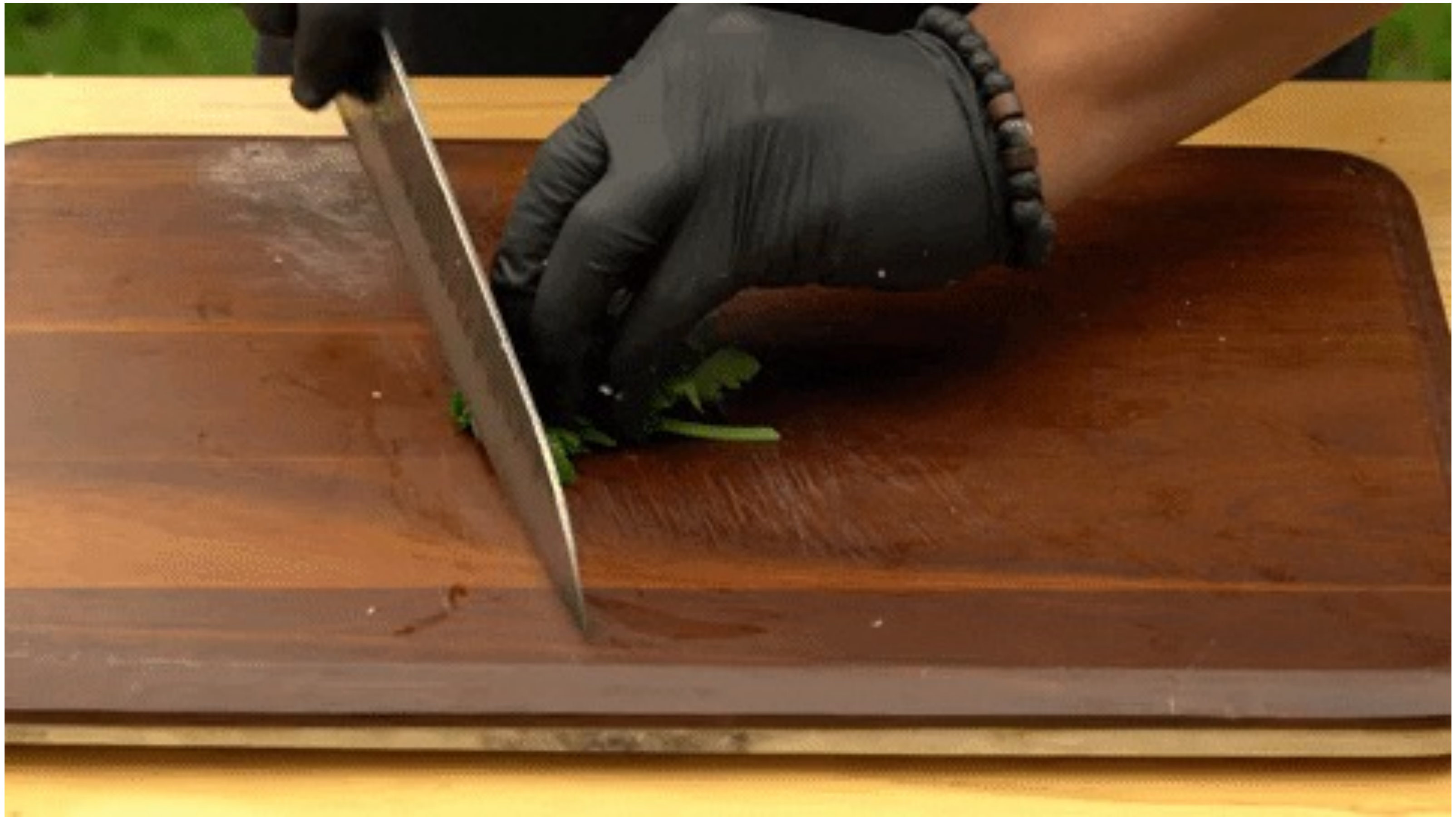


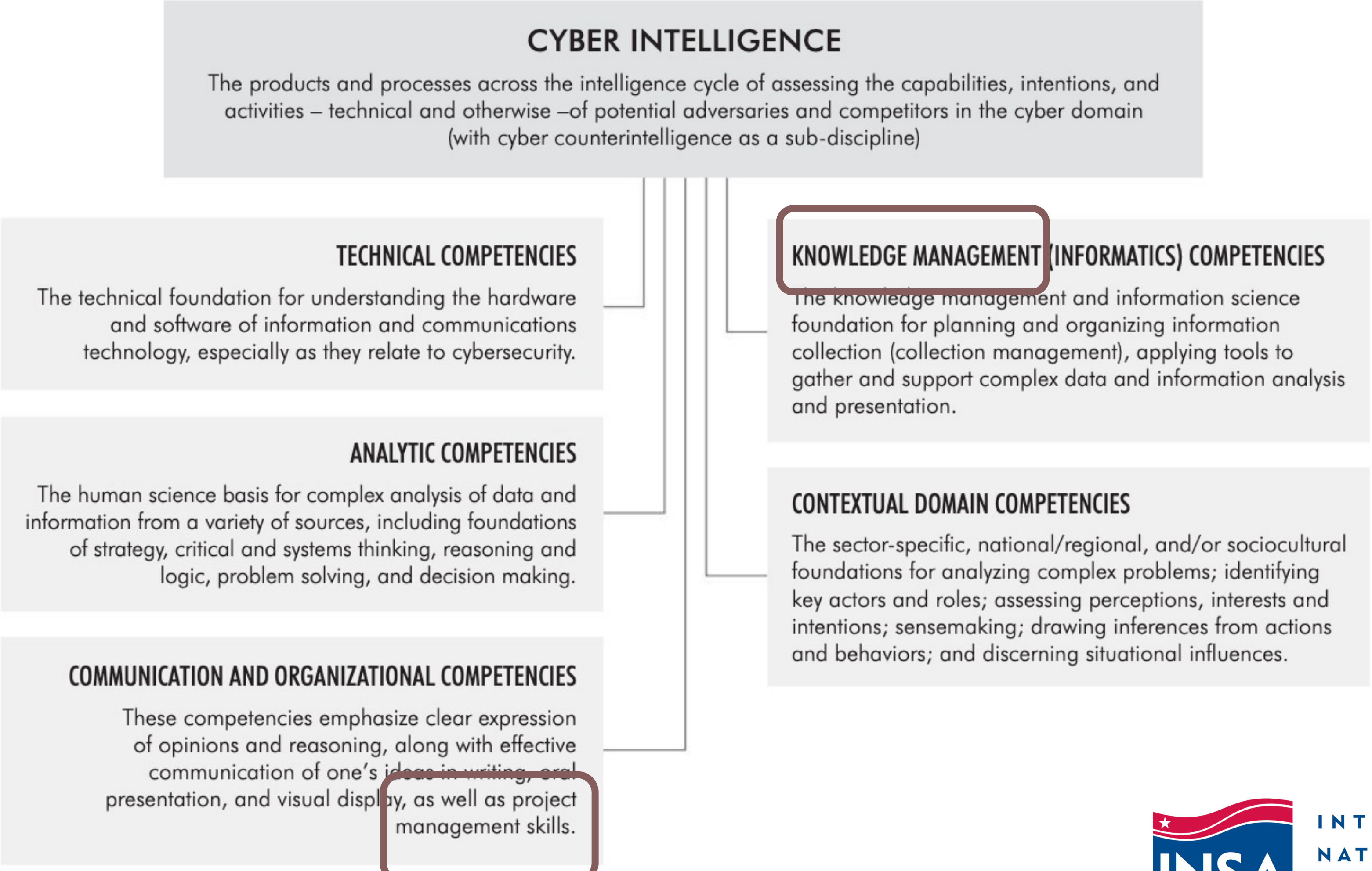
Image from bestofspain.es

THE BEST RUN

IMPORTANT THINGS ARE (SOMETIMES) BORING



CTI ANALYST SKILLSET



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.

INSA

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

A BASIC STEP

WHAT IF I TOLD YOU
THAT WORKFLOW AND CASE MANAGEMENT WOULD HELP YOUR TEAM
imgflip.com

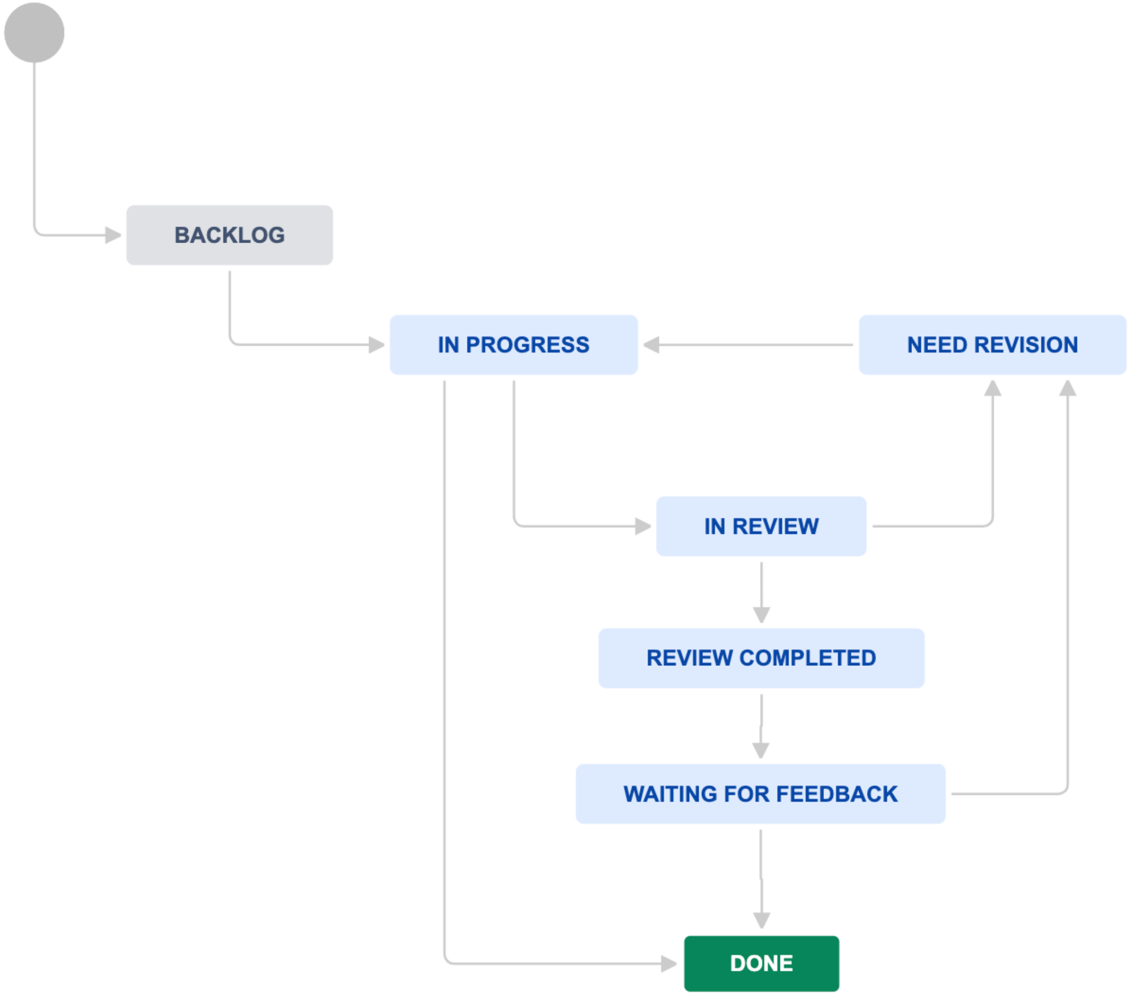
WHY WORKFLOW AND CASE MANAGEMENT?

Workflow, Coordination, and Collaboration

Knowledge Management

Metrics

WORKFLOW, COORDINATION & COLLABORATION



BACKLOG

IN PROGRESS

NEED REVISION

IN REVIEW

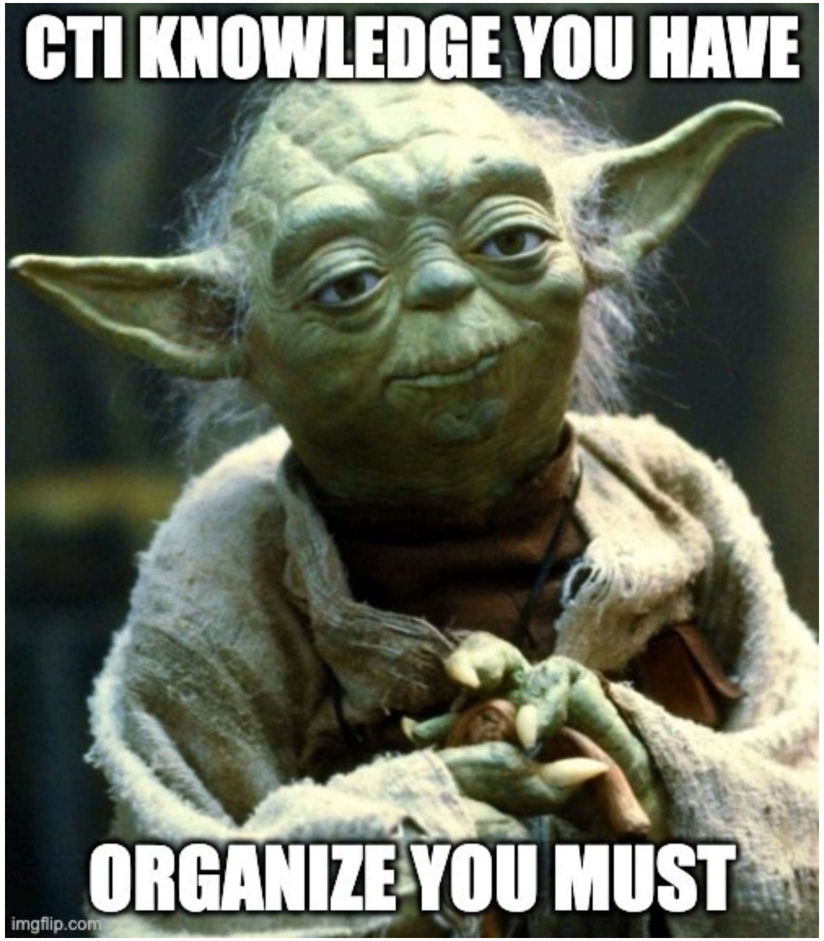
REVIEW COMPLETED

WAITING FOR FEEDBACK

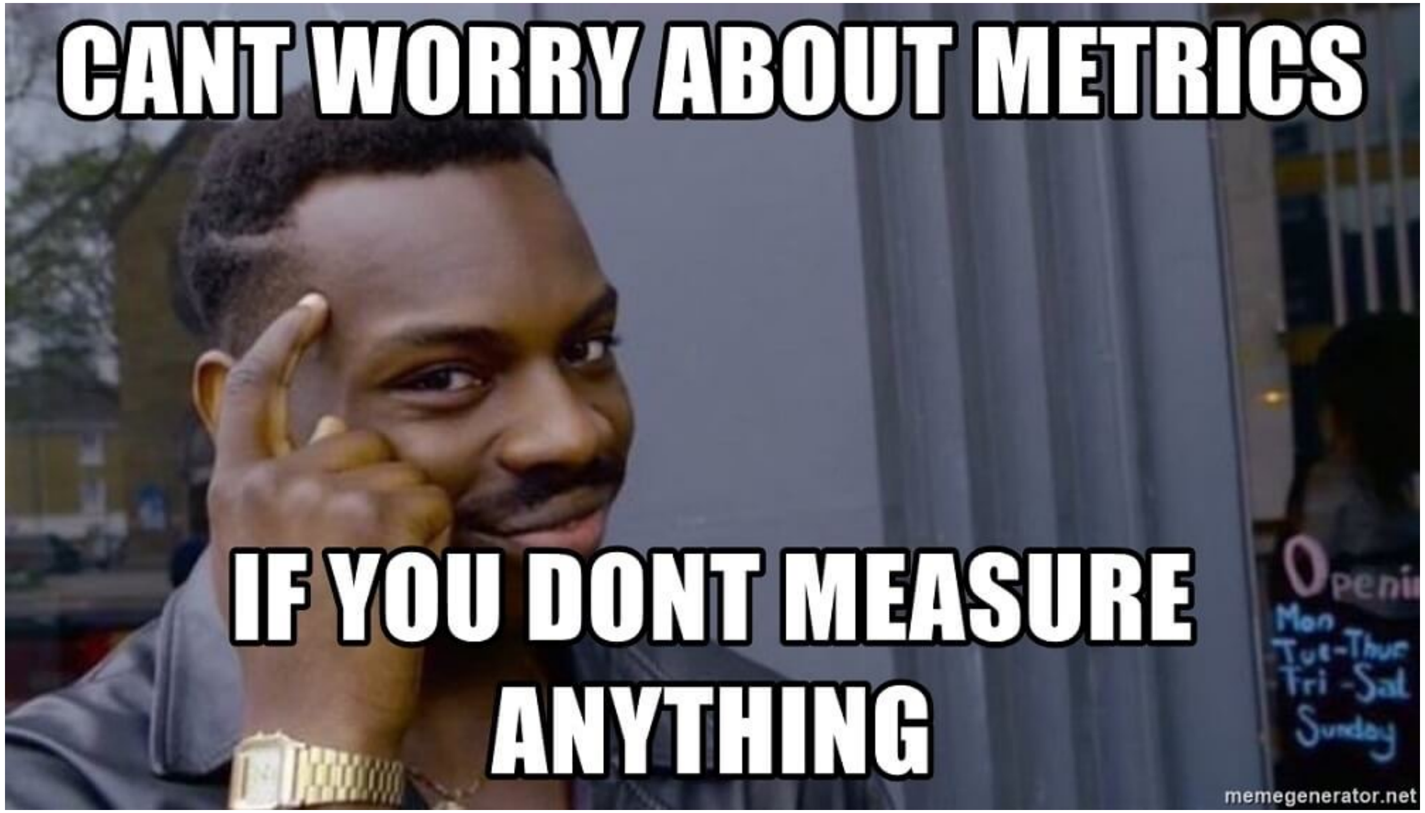
DONE

KNOWLEDGE MANAGEMENT

- Tagging
- Custom fields
- Easy searching and filtering
- Source rating
- Access control



WHAT GETS MEASURED, GETS MANAGED



MANAGEMENT METRICS

- Threats per criticality/impact level
- Time spent per PIR
- CTI assessments per threat type/threat actor
- CTI assessments (or time spent) supporting IR
- Quantitative feedback received per PIR
- Time spent on RFIs per stakeholder
- #hunts / #incidents from CTI assessments

TEAM METRICS

- Sources mostly used per PIR
- CTI deliverables per PIR
- CTI deliverables per stakeholder
- Average time spent per CTI deliverable
- CTI analysts' workload
- Average time spent in each phase of the workflow
- Time spent on CTI projects

WORKFLOW AND CASE MANAGEMENT FOR CTI
SO HOT RIGHT NOW
imgflip.com

Image from heritage-history.com

BASIC INGREDIENTS

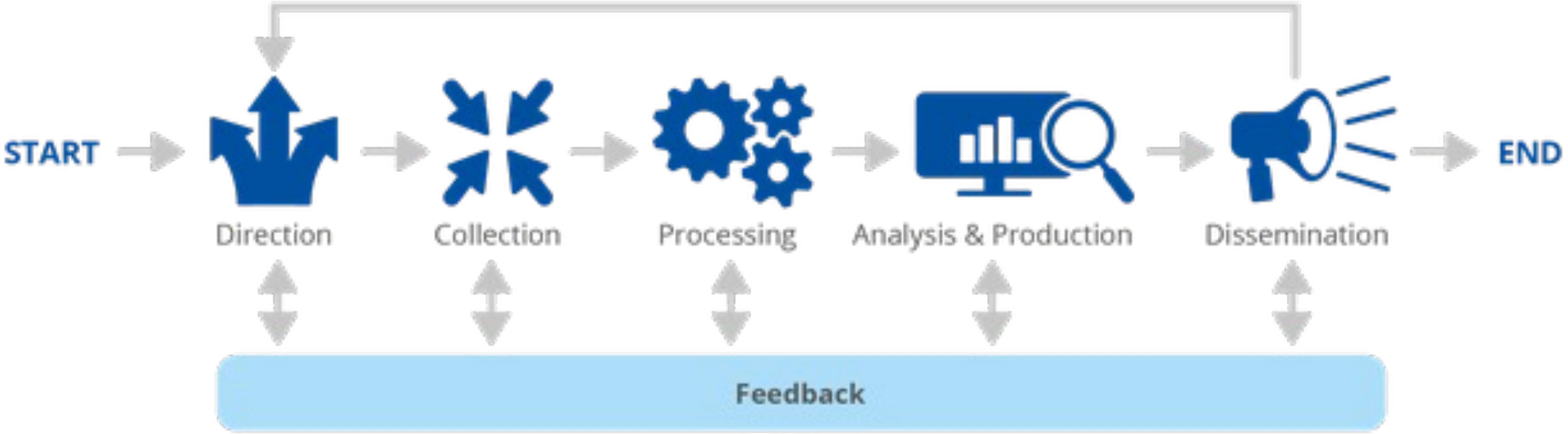
THE BEST RUN SAP

DOCUMENTATION MATTERS

Remember

- Data into buckets
- Consistency is key
- Spend time to save time

WHAT'S YOUR CTI PROCESS?



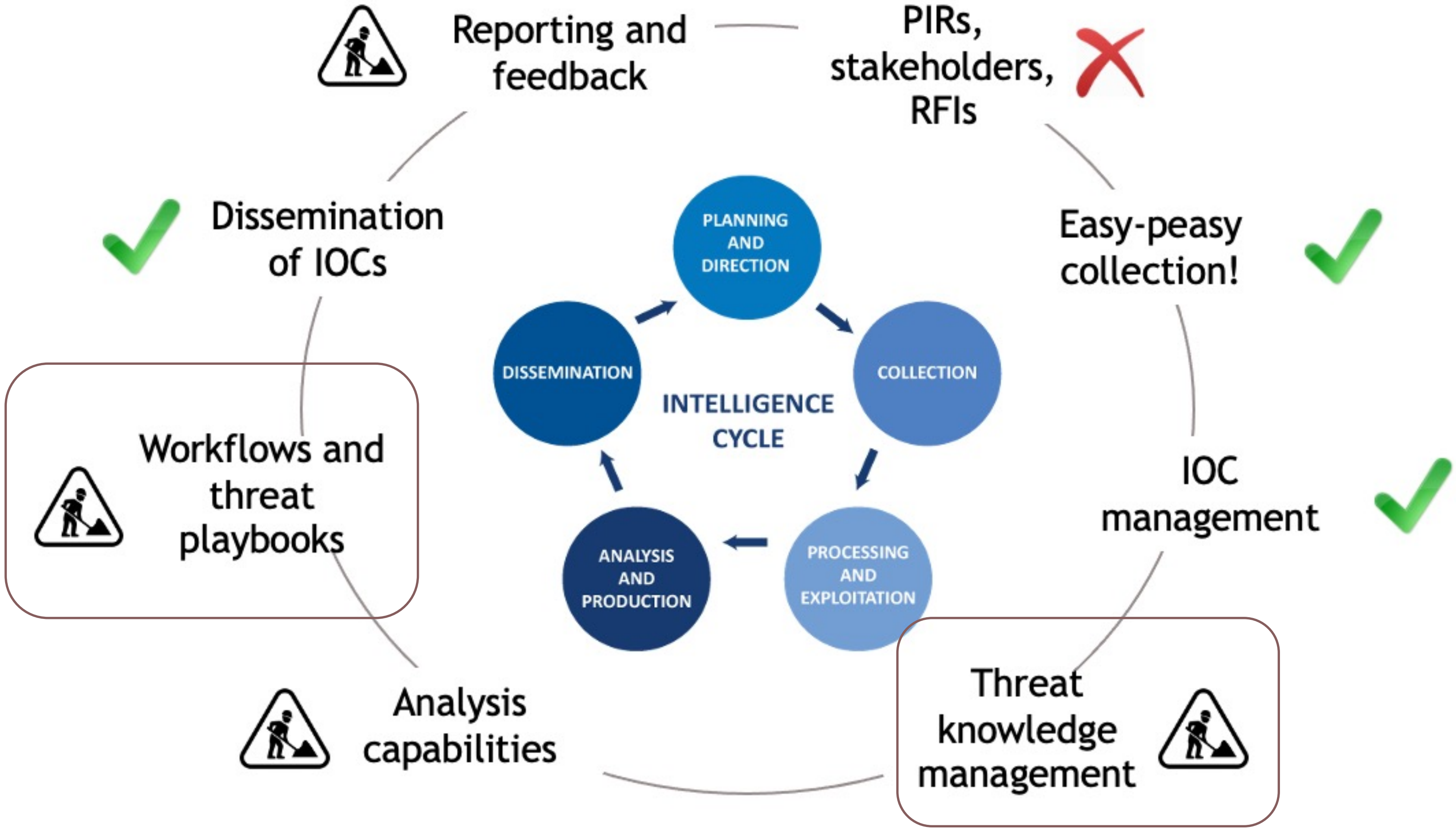
enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA
CYBERSECURITY
THREAT LANDSCAPE
METHODOLOGY

JULY 2022

TECHNOLOGY ENABLEMENT (1)



PIRs, stakeholders, RFIs ✗

Easy-peasy collection! ✓

IOC management ✓

Threat knowledge management ⚠

Analysis capabilities ⚠

Workflows and threat playbooks ⚠

Dissemination of IOCs ✓

Reporting and feedback ⚠

*SANS CTI Summit 2021

TECHNOLOGY ENABLEMENT (2)

SharePoint

JIRA

Confluence

Azure DevOps

servicenow

reqfast

Some TIPs

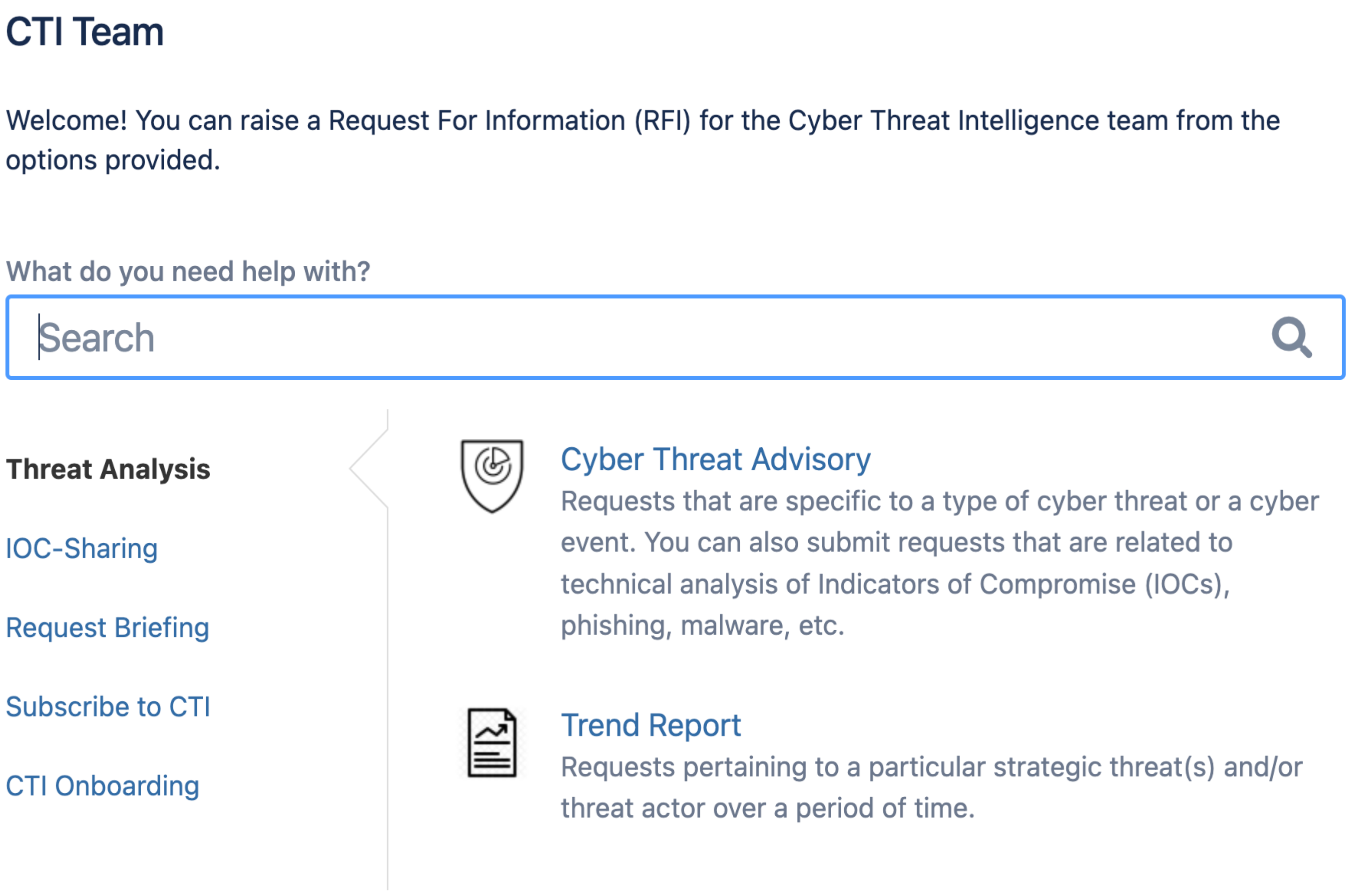
Recommendation is to live off the land (at least at the start of your CTI journey)

CTI ONE STOP SHOP

- Who you are / Contact Info
- Team’s Scope
- Intelligence Requirements
- CTI Report Library / CTI Blog
- Request For Information (RFI)

REQUEST FOR INFORMATION (1)

REQUEST FOR INFORMATION (2)



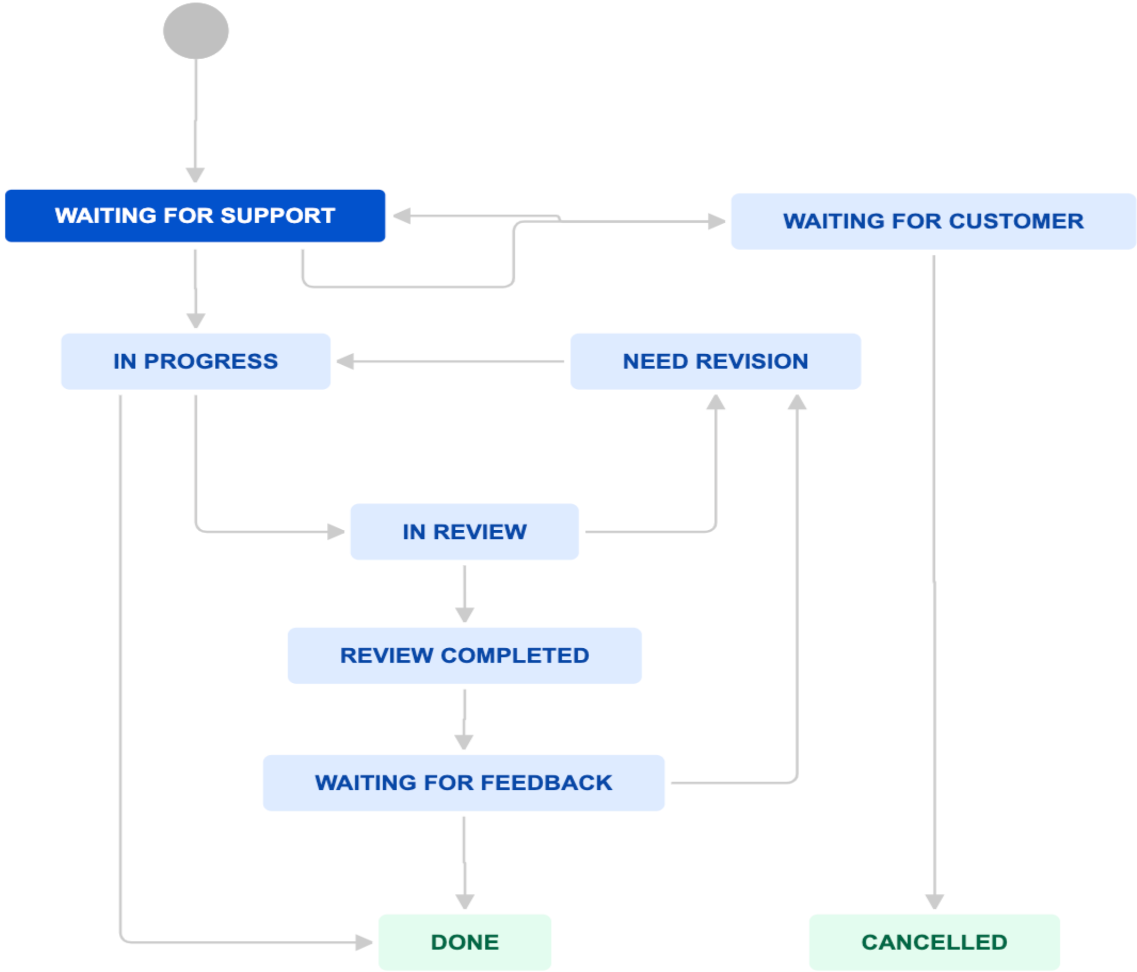
CTI Team

Welcome! You can raise a Request For Information (RFI) for the Cyber Threat Intelligence team from the options provided.

Cyber Threat Advisory
Requests that are specific to a type of cyber threat or a cyber event. You can also submit requests that are related to technical analysis of Indicators of Compromise (IOCs), phishing, malware, etc.

Trend Report
Requests pertaining to a particular strategic threat(s) and/or threat actor over a period of time.

REQUEST FOR INFORMATION (3)



THE BEST RUN SAP

CTI CHEF APPROVES

FINAL REMARKS

Image from elladocomicodedonquijote.wordpress.com

THE BEST RUN SAP

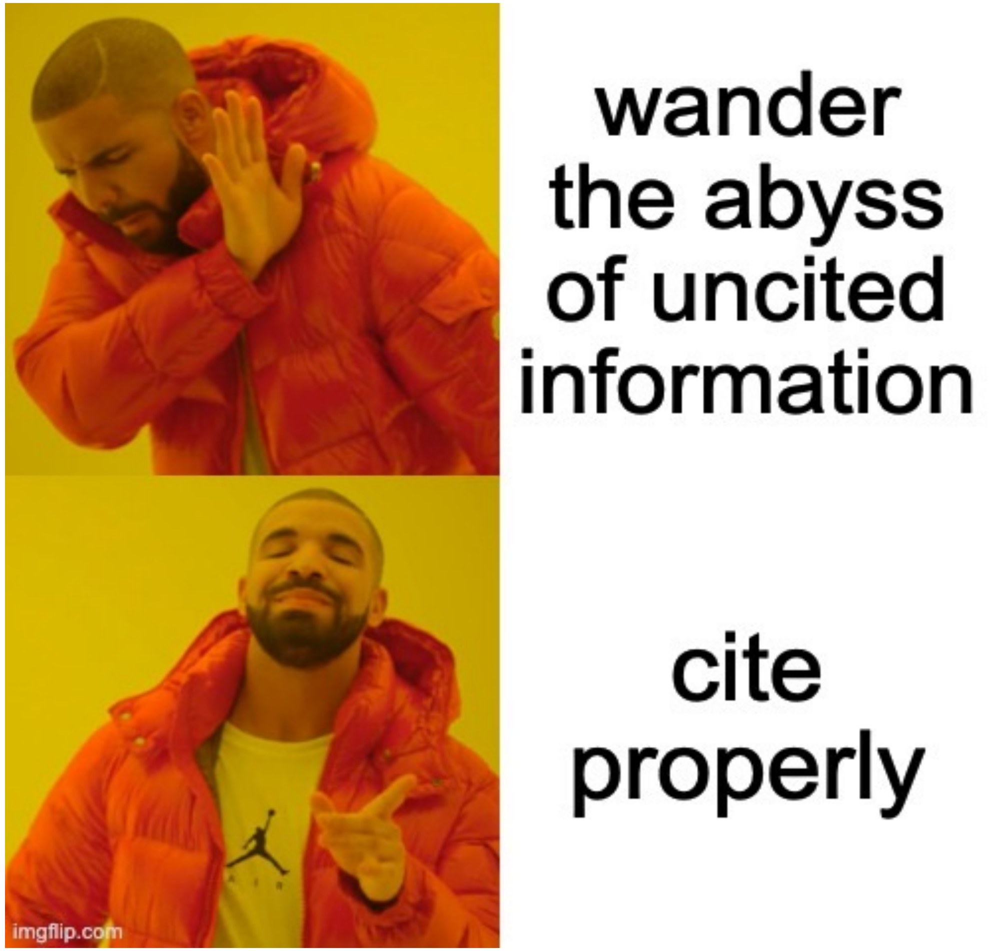
FINAL REMARKS

- Operationalizing the CTI process is a common challenge

- The importance of workflow and case management

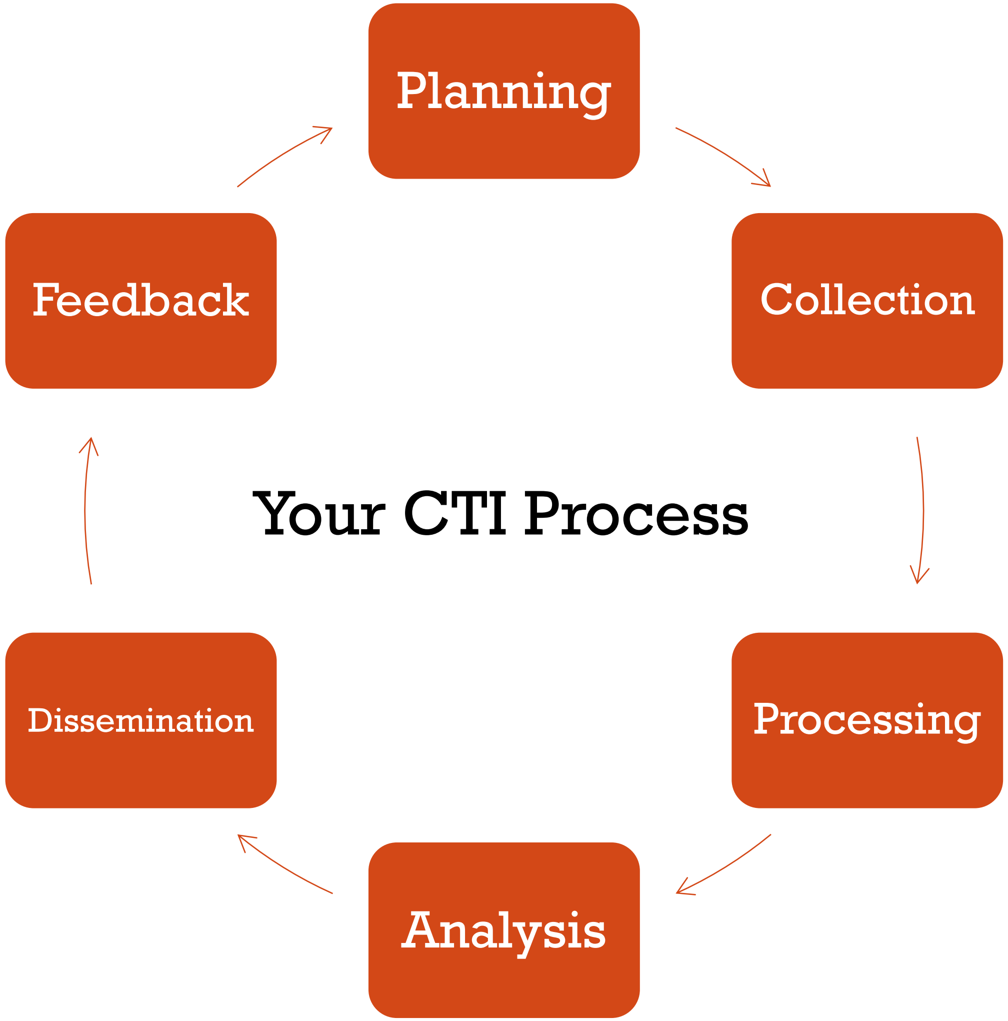
- The basic ingredients

REFERENCES



https://bit.ly/firstcti23

SPIN IT ROUND!


Planning

Collection

Processing

Analysis

Dissemination

Feedback

Your CTI Process

THANK YOU!

Andreas Sfakianakis

@asfakian

threatintel.eu

TLP:CLEAR