



TECHNOLOGY ENABLEMENT IN THE INTELLIGENCE CYCLE (AND THE ROLE OF TIPs)

ANDREAS SFAKIANAKIS

CTI-EU 2020





HOW CAN TECHNOLOGY HELP CTI
ANALYSTS?

WHAT IS HAPPENING TODAY AND
HOW CAN WE IMPROVE?

PROBLEM STATEMENTS

WHO AM I

- CTI in Financial and Oil & Gas sectors
- ENISA CTI, FIRST.org CTI, European Commission
- Twitter: @asfakian
- Website: www.threatintel.eu



DISCLAIMER

- Original authors are referenced within the slide deck.
- References for this presentation: <http://bit.ly/ctieu2020>
- This is a vendor agnostic presentation
- Views are my own

OUTLINE

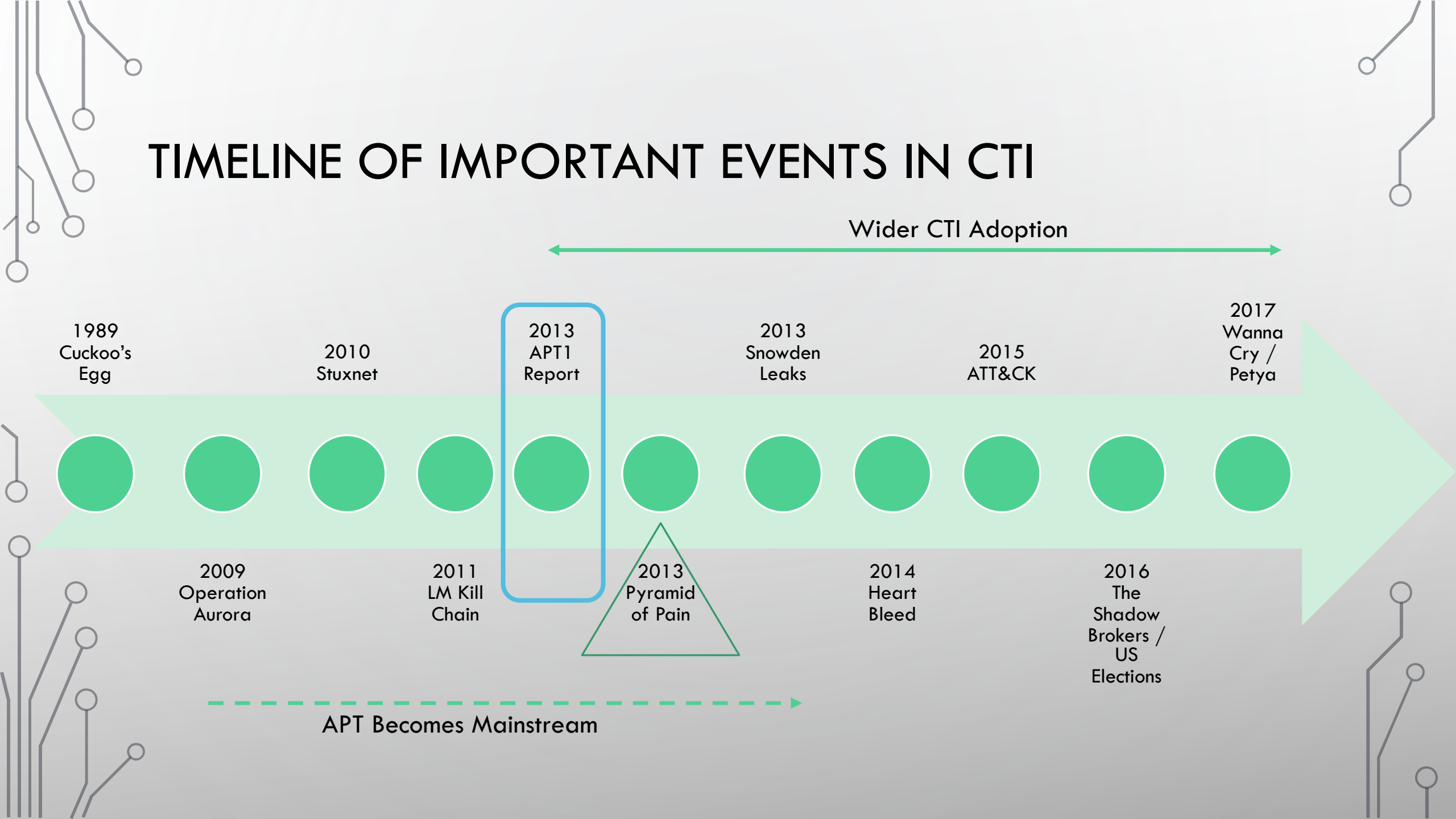
- Setting the scene
- Technology enablement in the CTI cycle
- From Excel to TIPs
- A study of TIPs
- Recommendations and opportunities
- Final remarks





SETTING THE SCENE

TIMELINE OF IMPORTANT EVENTS IN CTI



1989
Cuckoo's
Egg

2010
Stuxnet

2013
APT1
Report

2013
Snowden
Leaks

2015
ATT&CK

2017
Wanna
Cry /
Petya

2009
Operation
Aurora

2011
LM Kill
Chain

2013
Pyramid
of Pain

2014
Heart
Bleed

2016
The
Shadow
Brokers /
US
Elections

APT Becomes Mainstream

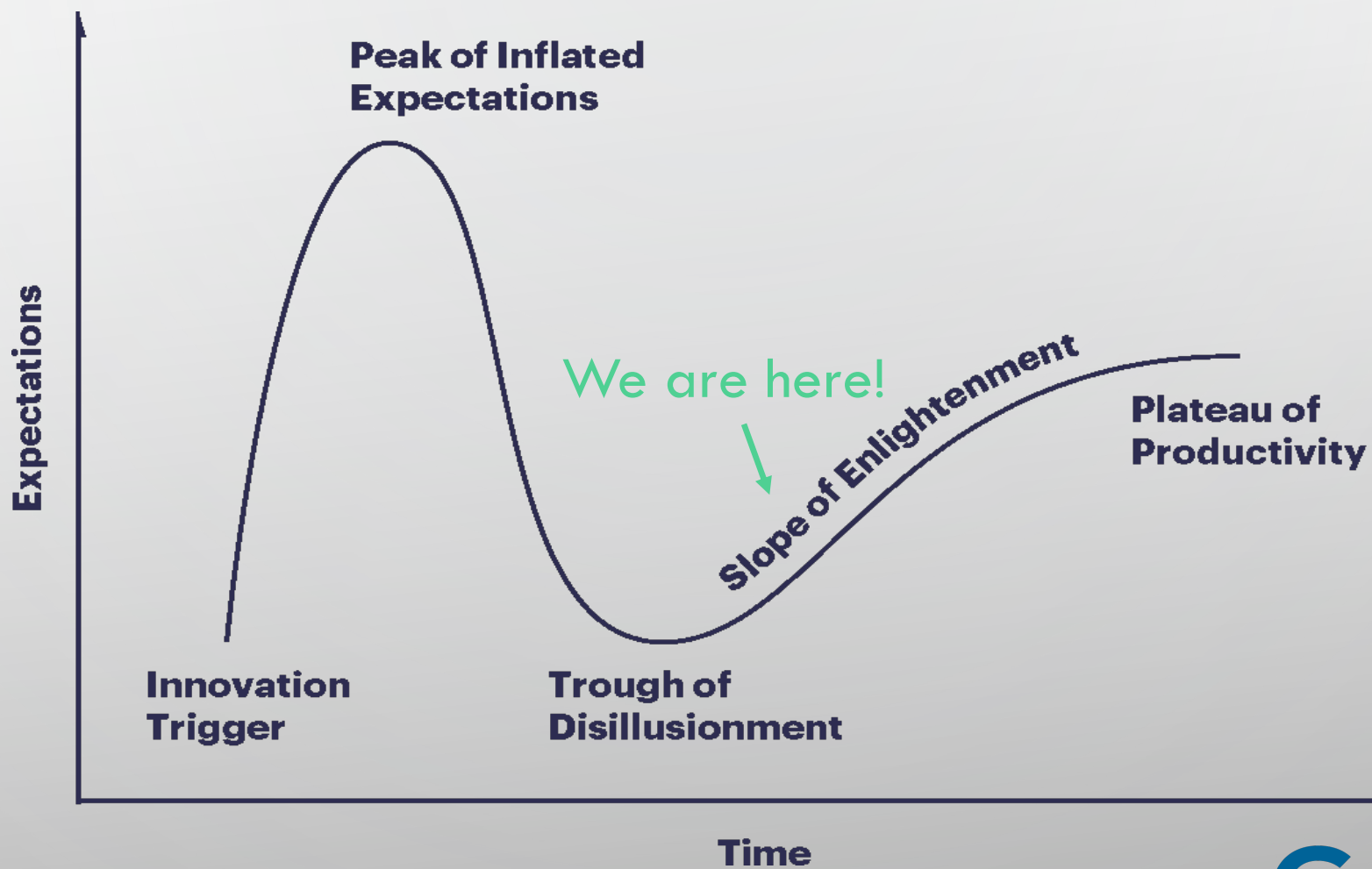
Wider CTI Adoption

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	Increasing technology enablement	Mature technology enablement	Mature technology enablement

Reference:

CTI HYPE CYCLE



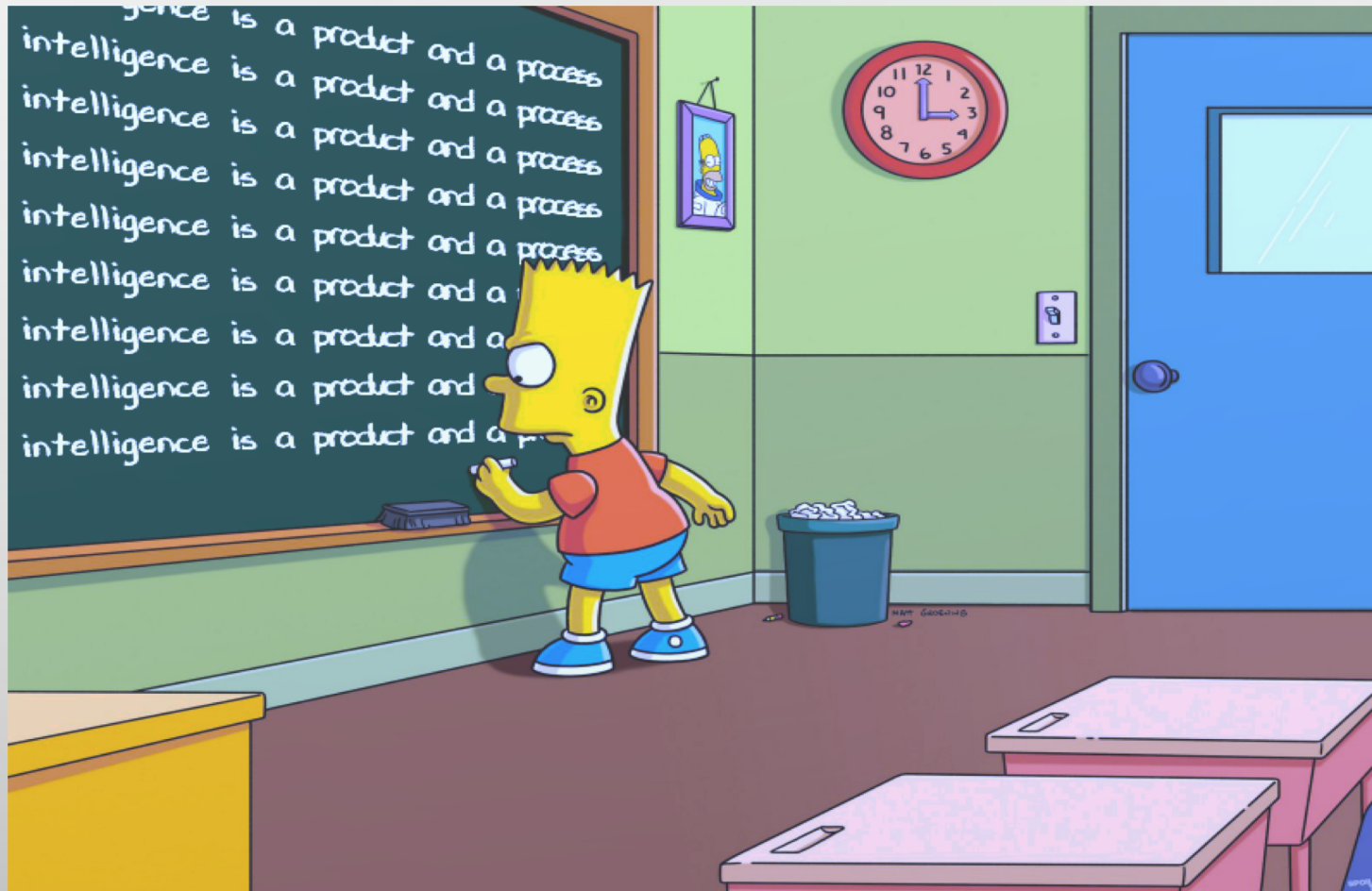
Reference:

Gartner®



TECHNOLOGY ENABLEMENT IN THE INTELLIGENCE CYCLE

CTI 101



INTELLIGENCE CYCLE



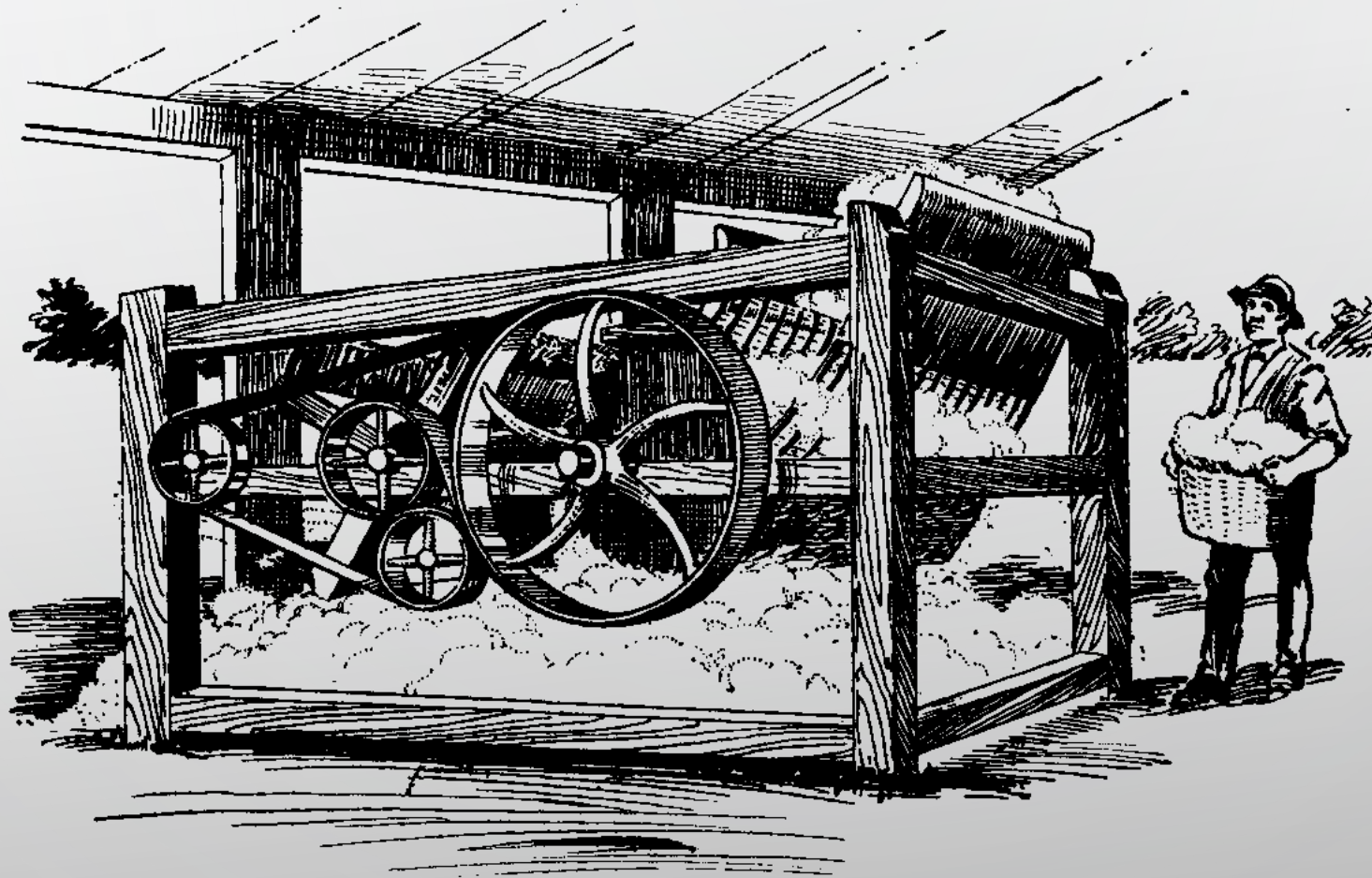
INTELLIGENCE DIRECTION



AT THE PARTING OF THE WAYS
A cartoon appearing in the May, 1919, *One Big Union* which speaks for itself.



INTELLIGENCE COLLECTION



PROCESSING AND EXPLOITATION



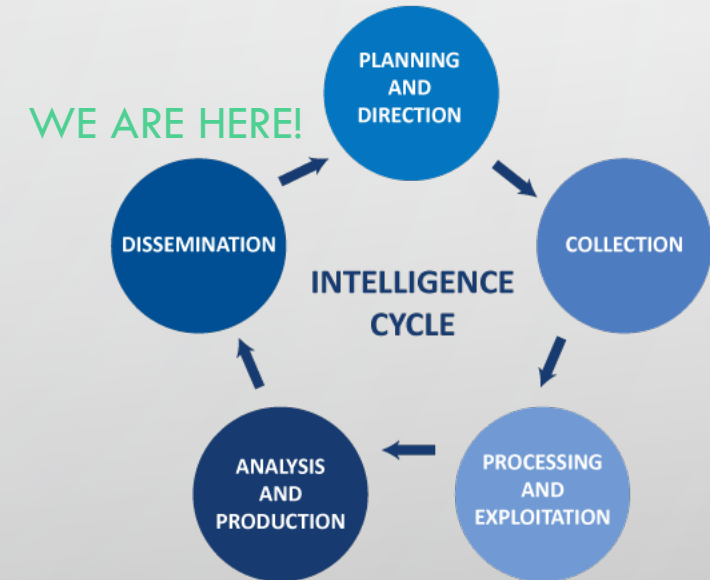
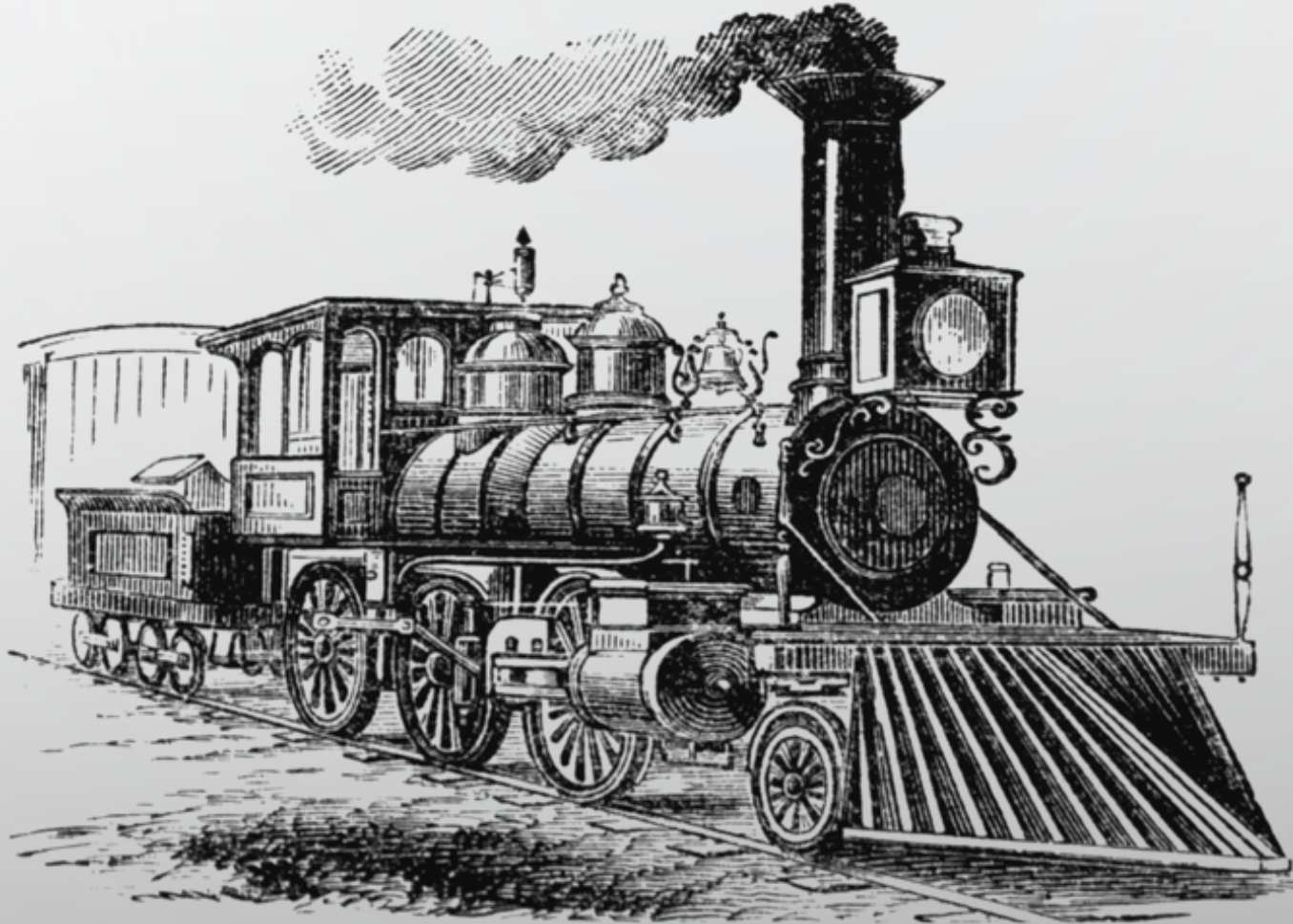
WE ARE
HERE!

ANALYSIS AND PRODUCTION



WE ARE HERE!

DISSEMINATION AND FEEDBACK



FUNCTIONAL REQUIREMENTS FOR TECHNOLOGY SUPPORTING CTI



Annex B: TIP functional requirements

Work in progress - Excel sheet to be published in March 2020!

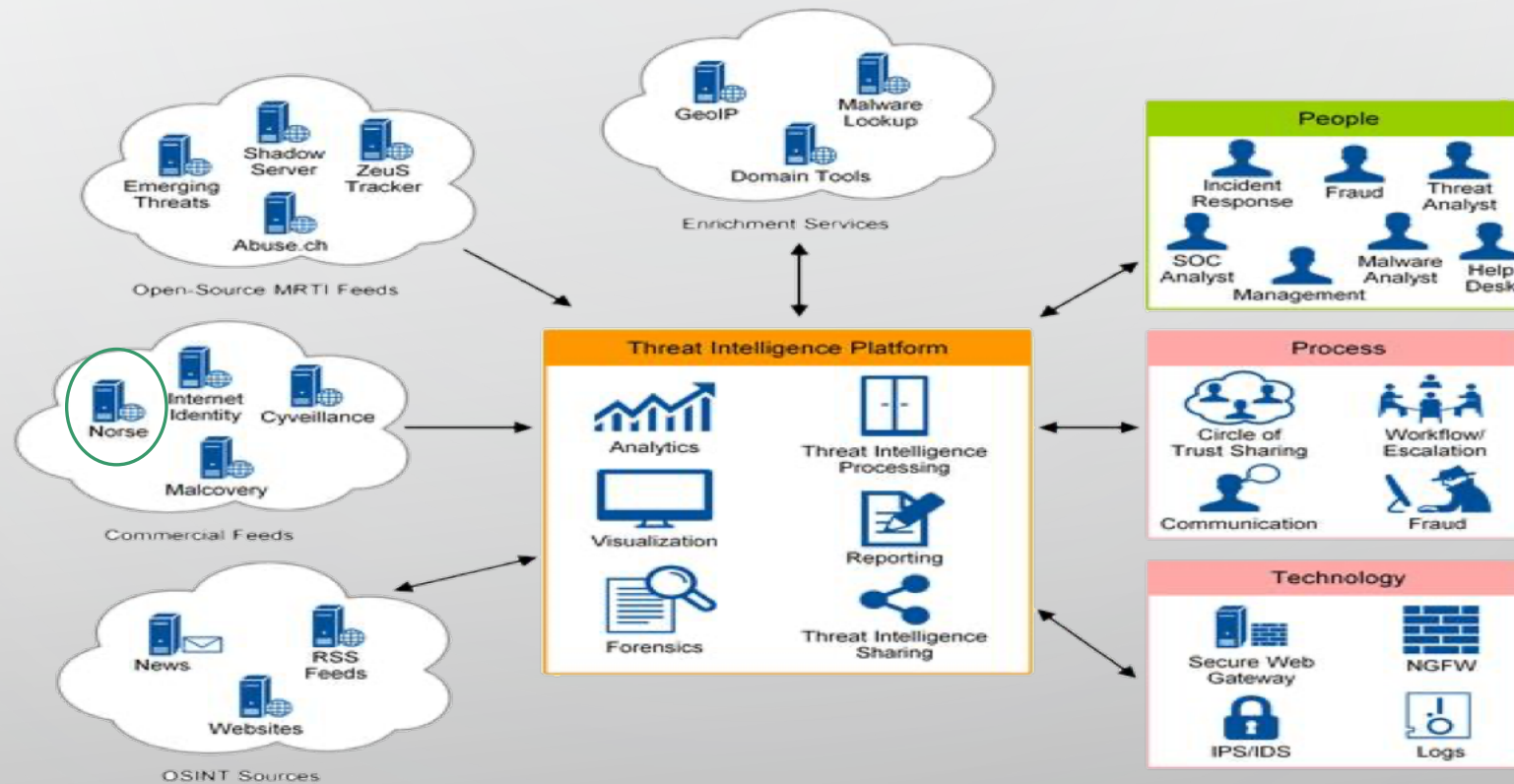
References for this presentation: <http://bit.ly/ctieu2020>



FROM EXCEL TO TIPs

WHAT IS A TIP?

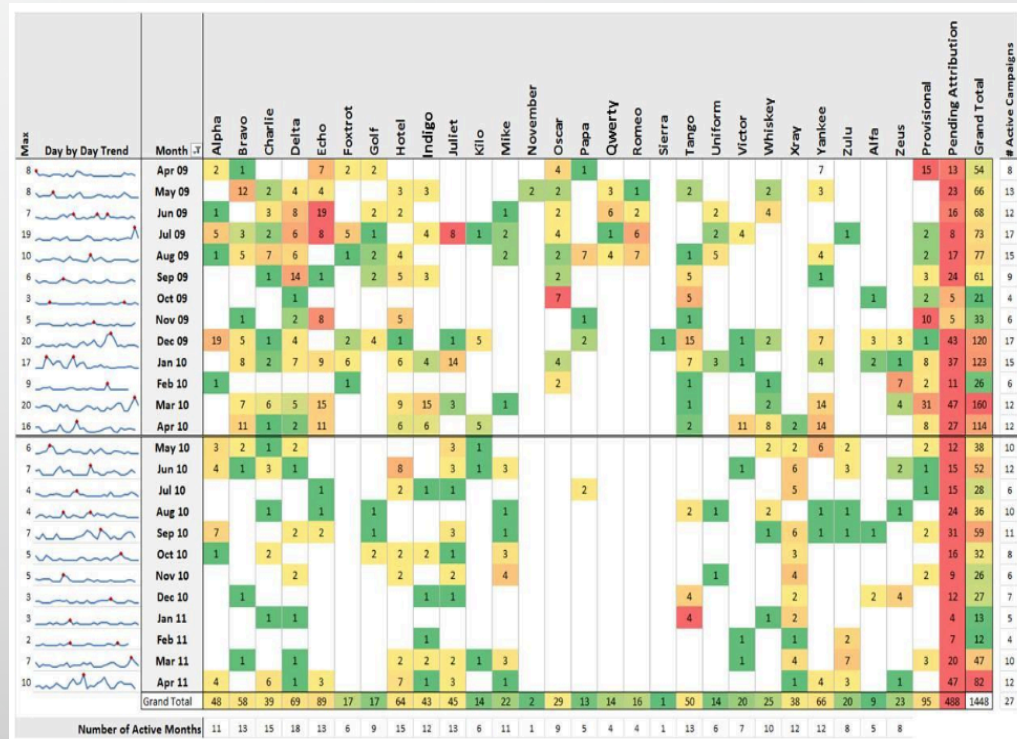
(2014 VERSION)



Reference:

Gartner

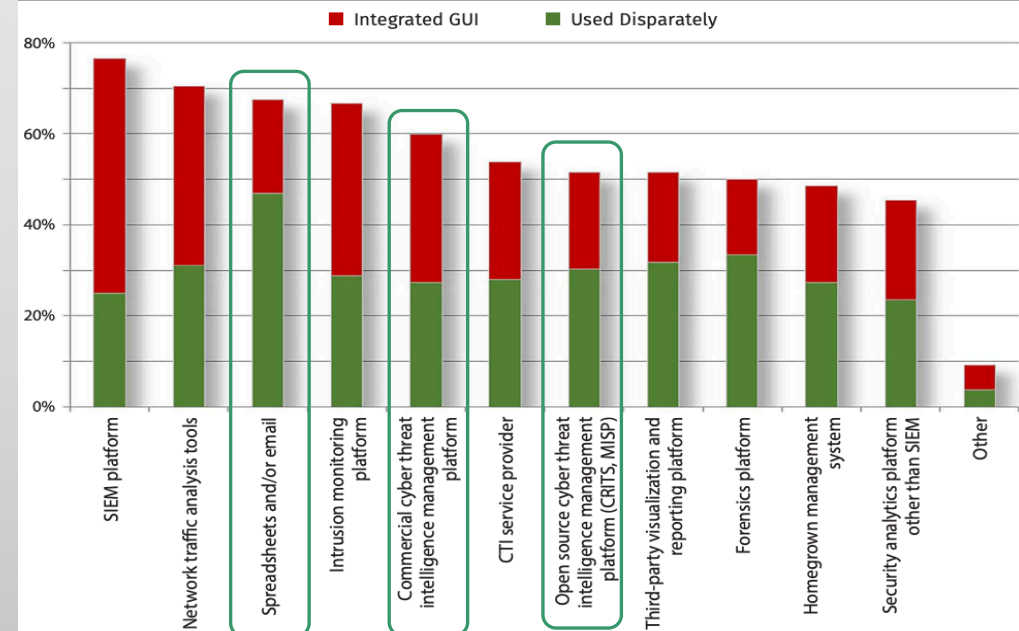
EXCEL THE FIRST TIP



Reference:

LOCKHEED MARTIN

What type of management tools are you using to aggregate, analyze and/or present CTI information? *Select all that apply, and indicate whether these are used disparately or work together under a unified GUI.*



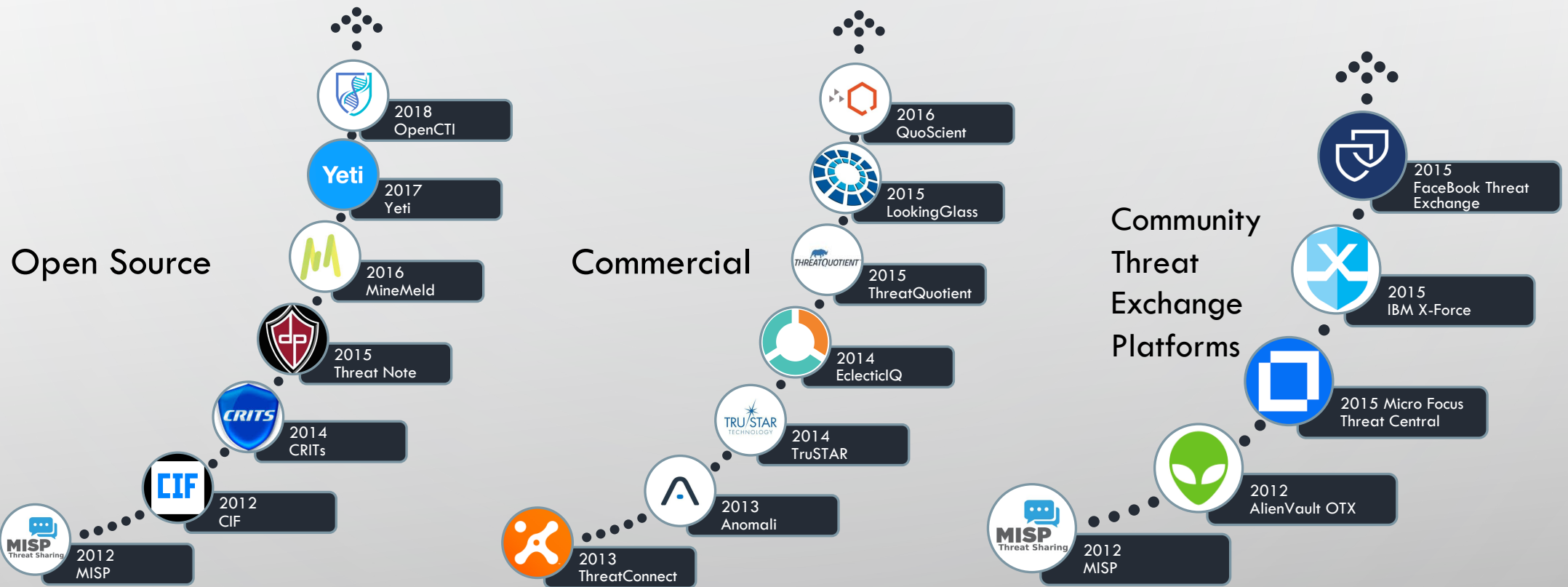
Reference:

SANS

DO YOU STILL THINK OF YOUR EX?



TIP LANDSCAPE



EXAMPLE COMPARISON OF OPEN SOURCE TIPs

Evaluated Criteria	MISP	CIF	CRITs	SE
Import/Export Format	●	○	●	—
Integration Capabilities	●	●	○	○
Data Exchange Std.	●	○	○	○
Support of Collaboration	●	●	○	○
Analysis Capabilities	○	○	●	○
Graph Generation	○	○	●	○
License	●	●	●	○
Hardware Requirements	●	—	●	●
—Low/Basic ○ Medium/Average ● High/Advanced				

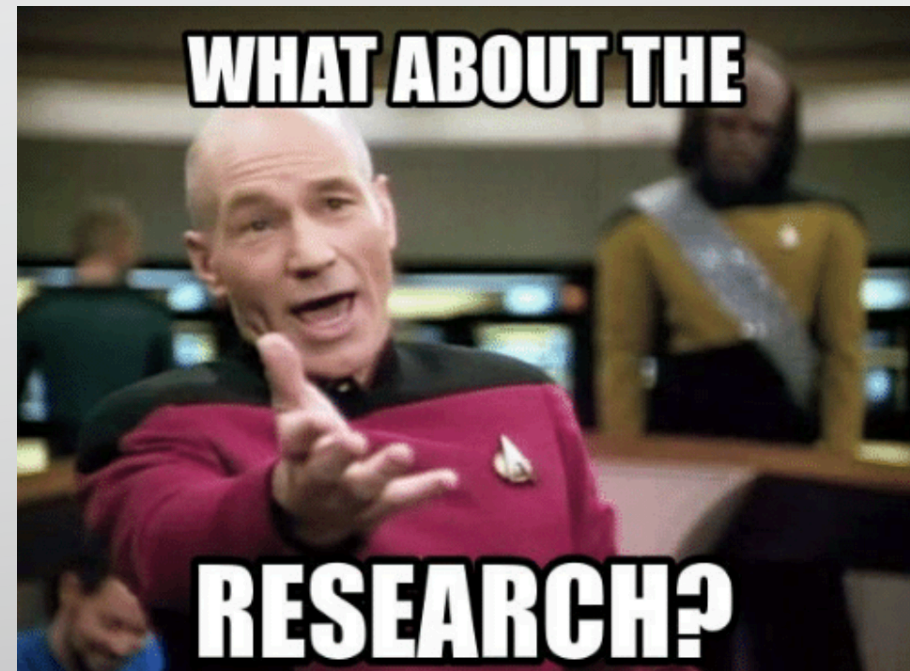
Reference: *Enriching Threat Intelligence Platforms Capabilities* (Secrypt2019)



A STUDY OF TIPs



PRIOR RESEARCH ON TIPs

- Gartner and Forrester
- TIP vendors' whitepapers
- Academic research
- CTI professionals' blogs and presos
- SANS and CMU SEI CTI surveys
- ENISA report on TIPs





LIMITATIONS OF CURRENT TIPs

- Focus on data collection
 - Voluminous shared threat data
 - Threat data issues
 - Limited analysis capabilities
 - Integration difficulties
 - Limited workflow enablement
 - Fragmentation of tools and threat knowledge
- 
- 



RECOMMENDATIONS AND OPPORTUNITIES

SELECTING THE RIGHT TIP FOR YOUR ORG (1 / 2)

- Identify YOUR requirements and use cases based on processes and routine RFls
- Focus on the problems and pain points and NOT on the technology solutions and their features
- Prioritize requirements and use cases (MuSCoW ratings, core requirements vs enhancements)
- Focus on analytical problems first
- Interview major internal stakeholders (e.g. procurement team, CTI team's stakeholders, etc.)
- Think also about non-functional requirements (e.g. support, integrations, on prem, etc.)
- Try an open source TIP if possible

SELECTING THE RIGHT TIP FOR YOUR ORG (2/2)

- Identify the evaluation criteria
 - Prioritized requirements and use cases
 - Demo, vendor training, quality of experience during PoC
 - Price
- TIP solution research
- Selection of the most relevant TIPs for PoC'ing
 - Scoring exercise after PoC
- Leadership communication and budget justification

RECOMMENDATIONS AND OPPORTUNITIES

- Organizations
- TIP Users
- TIP Developers and Vendors
- Intelligence Producers
- CTI Community and Researchers



TIP FOR EU CSIRT COMMUNITY AND ISACs

- MeliCERTes (SMART 2018/1024)
 - NASK/CERT.pl
 - nic.at/CERT.at
 - CERT.EE
 - CIRCL
 - Deloitte
- ISACs (SMART 2018/1022)
 - Gapgemini
 - Spark Legal Network
 - TNO
 - DFN-CERT



THE FUTURE OF TIPs





FINAL REMARKS

FINAL REMARKS

- TIP has a central role in CTI analyst's toolset (not necessarily a single pane of glass)
- Use diverse technology to support cyber intelligence
- Select your toolsets wisely based on YOUR requirements and use cases
- Build technology around processes and not processes around technology
- Adopt SOAR capabilities to assist with workflow, automation and threat analysis playbooks
- Help the community and drive the vendors
- Closely monitor this emerging technology area

THANKSGIVING SLIDE

ENISA

Razvan Gavrilă

Chris Beard

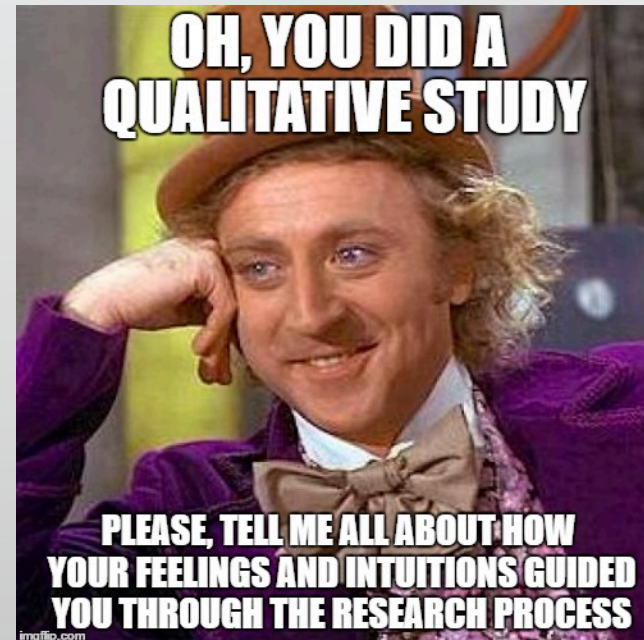
Sarah Brown

Alexandre Dulaunoy

Jane Ginn

Pasquale Stirparo

Omid Raghimi



THANK YOU

ANDREAS SFAKIANAKIS

@asfakian

References for this presentation: <http://bit.ly/ctieu2020>

