Still thinking about your Ex(cel)? Here are some TIPs

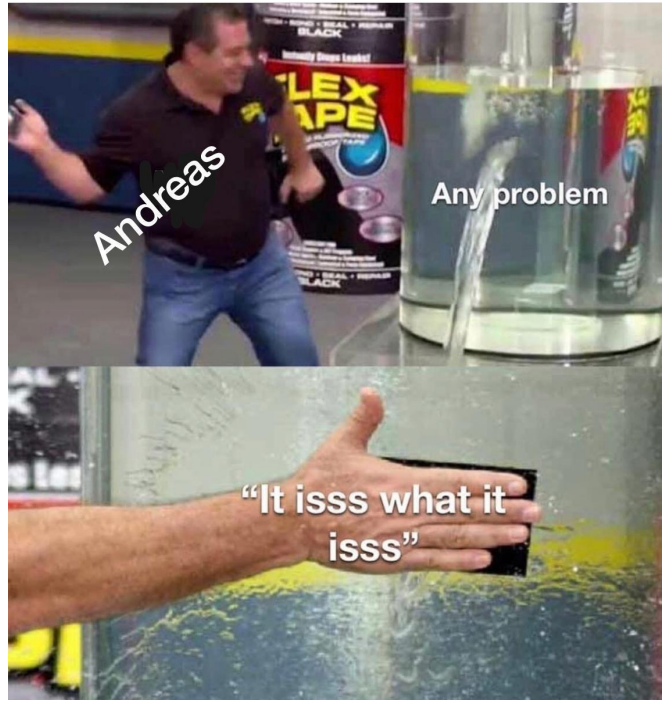
The past, present, and future of Threat Intelligence Platforms (TIPs)

Andreas Sfakianakis

SANS CTI Summit 2021

who am I

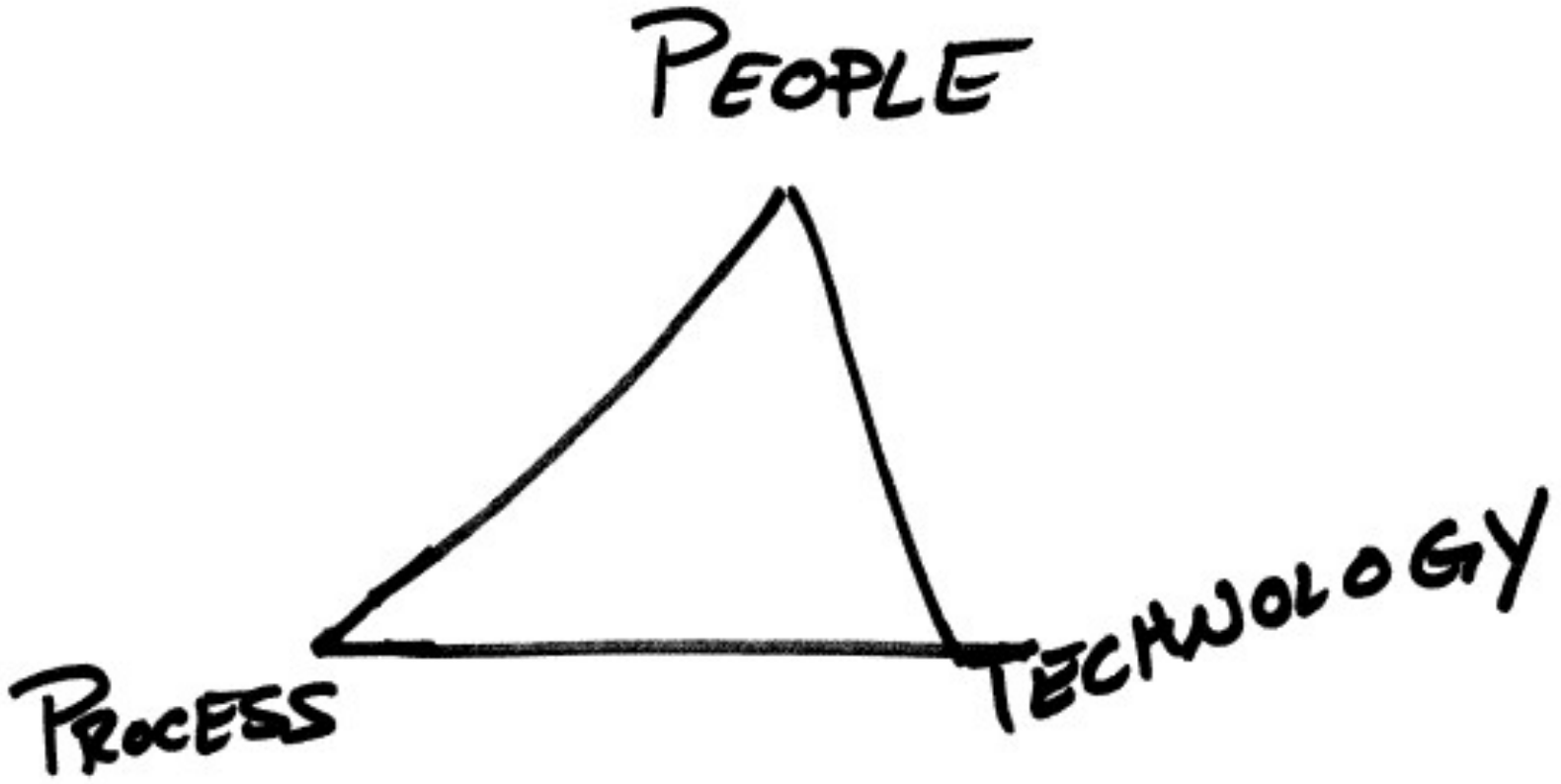
- CTI Lead EMEA @ S&P Global
- CTI @ Financial and Oil & Gas sectors
- ENISA, FIRST.org, SANS, European Commission
- Twitter: @asfakian Website: www.threatintel.eu



Disclaimer

- Original authors are referenced within the slide deck
- Resources for this presentation: https://bit.ly/ctisummit2021
- This is a vendor agnostic presentation
- Views are my own

What about technology supporting CTI operations?



Outline

The brief history of TIPs

Current state of TIPs

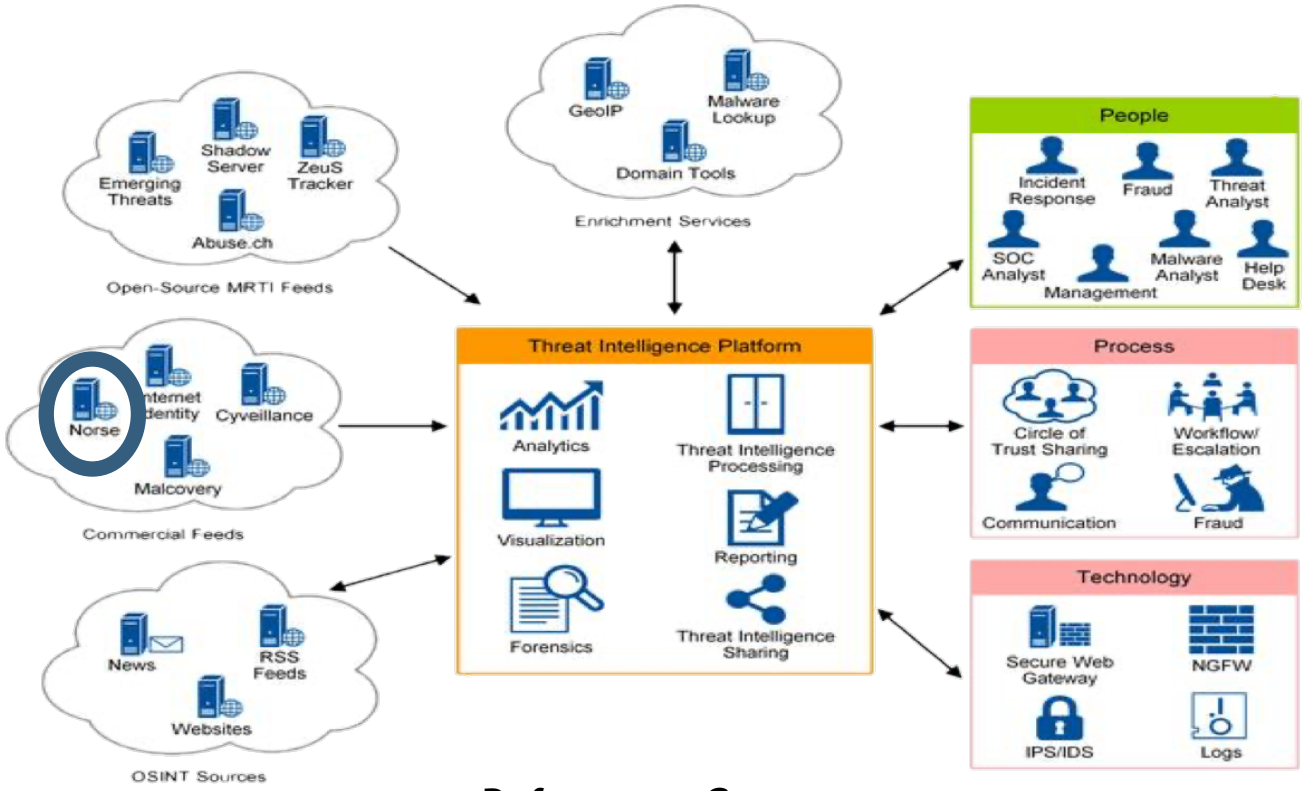
Looking ahead

The brief history of TIPs

(Past)

What is a Threat Intelligence Platform (TIP)?

(2014 version)



Reference: Gartner

- IOCs -> TIP -> security stack
- Threat team knows!
- Enrich and analyze all the things!?
- Share! Share! Share!
- Intelligence lifecycle support

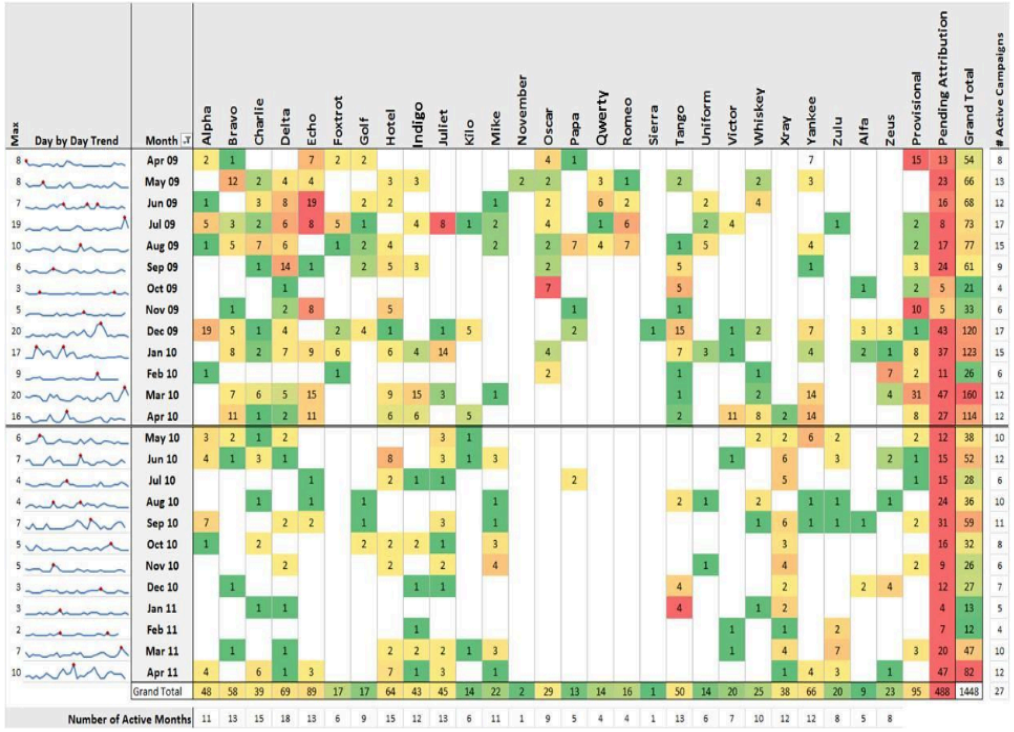
TIP landscape

Open Source

Commercial

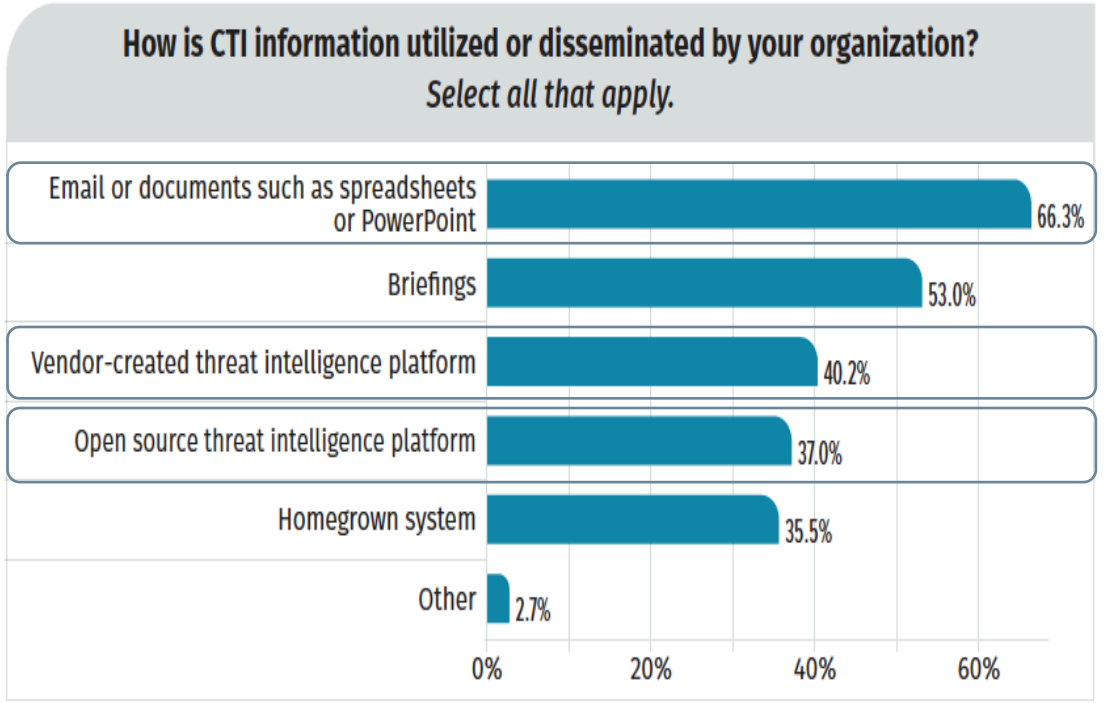
Community Exchange Platforms

Excel the first TIP



Max	Day by Day Trend	Month	Alpha	Bravo	Charlie	Delta	Echo	Foxtrot	Golf	Hotel	Indigo	Juliet	Kilo	Mike	November	Oscar	Papa	Qwerty	Romeo	Sierra	Tango	Uniform	Victor	Whiskey	Xray	Yankee	Zulu	Alfa	Zeus	Provisional	Pending Attribution	Grand Total	# Active Campaigns
8		Apr 09	2	1			7	2	2							4	1								7				15	13	54	8
8		May 09		12	2	4	4			3	3				2	2		3	1		2			2	3					23	66	13
7		Jun 09	1		3	8	19		2	2				1		2		6	2			2		4						16	68	12
19		Jul 09	5	3	2	6	8	5	1		4	8	1	2		4		1	6			2	4				1			2	8	73	17
10		Aug 09	1	5	7	6		1	2	4				2		2	7	4	7		1	5				4				2	17	77	15
6		Sep 09			1	14	1		2	5	3					2					5				1					3	24	61	9
3		Oct 09				1										7					5						1			2	5	21	4
5		Nov 09		1		2	8			5							1				1									10	5	33	6
20		Dec 09	19	5	1	4		2	4	1		1	5				2			1	15		1	2		7		3	3	1	43	120	17
17		Jan 10		8	2	7	9	6		6	4	14				4					7	3	1			4		2	1	8	37	123	15
9		Feb 10	1					1								2					1			1					7	2	11	26	6
20		Mar 10		7	6	5	15			9	15	3		1							1			2		14			4	31	47	160	12
16		Apr 10		11	1	2	11			6	6		5								2		11	8	2	14				8	27	114	12
6		May 10	3	2	1	2						3	1											2	2	6	2			2	12	38	10
7		Jun 10	4	1	3	1				8		3	1	3									1		6		3		2	1	15	52	12
4		Jul 10				1				2	1	1					2								5					1	15	28	6
4		Aug 10			1		1		1					1							2	1		2		1	1		1		24	36	10
7		Sep 10	7			2	2		1			3		1										1	6	1	1	1		2	31	59	11
5		Oct 10	1		2				2	2	2	1		3											3						16	32	8
5		Nov 10				2				2		2		4								1			4					2	9	26	6
3		Dec 10		1							1	1									4				2			2	4		12	27	7
3		Jan 11			1	1															4			1	2						4	13	5
2		Feb 11									1												1		1		2				7	12	4
7		Mar 11		1		1				2	2	2	1	3									1		4		7			3	20	47	10
10		Apr 11	4		6	1	3			7	1	3		1											1	4	3		1		47	82	12
		Grand Total	48	58	39	69	89	17	17	64	43	45	14	22	2	29	13	14	16	1	50	14	20	25	38	66	20	9	23	95	488	1448	27
		Number of Active Months	11	13	15	18	13	6	9	15	12	13	6	11	1	9	5	4	4	1	13	6	7	10	12	12	8	5	8				

Reference: Lockheed Martin

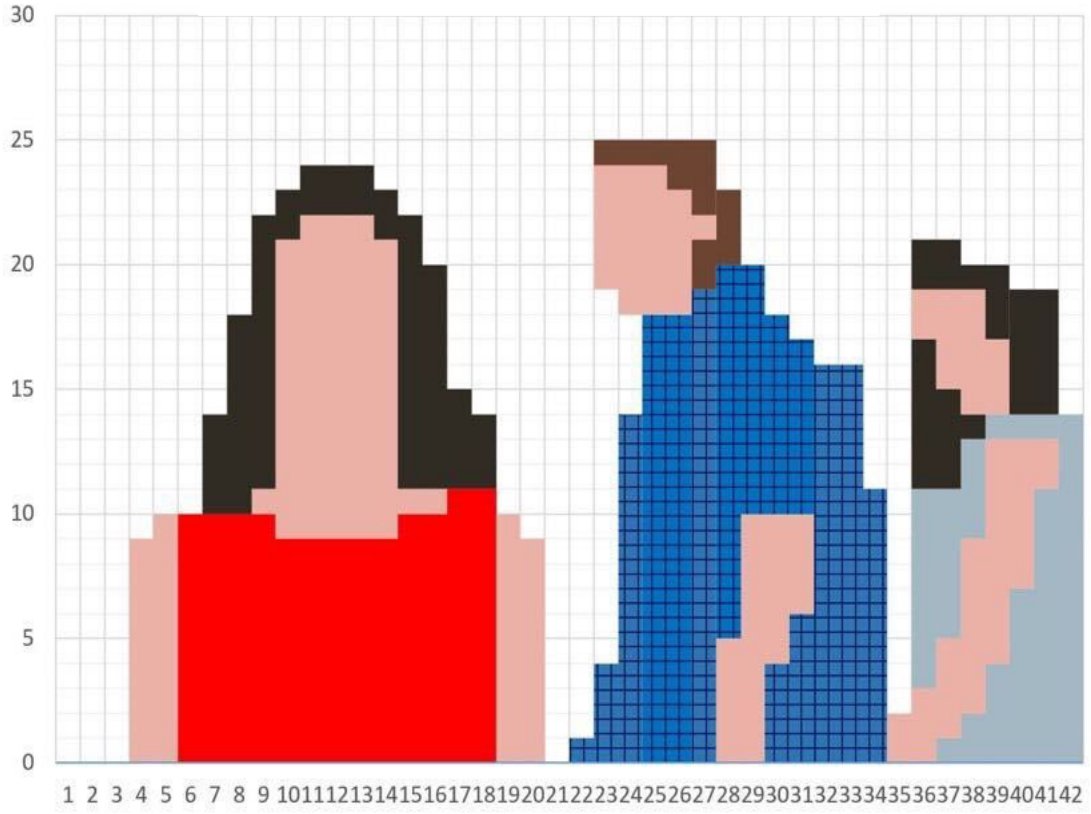


Reference: SANS

Do you still think about your ex?

Reference: https://twitter.com/_daviant/status/1253039113151938562

Do you still think about your ex?



Reference: https://twitter.com/_daviant/status/1253039113151938562

Recap
The brief history of TIPs

- Emerging technology with loose definition
- Different shades of TIPs
- Variety of management tools to support CTI

The TIP is the quarterback that orchestrates your intelligence work.

Reference: Rick Holland

Resources
The brief history of TIPs

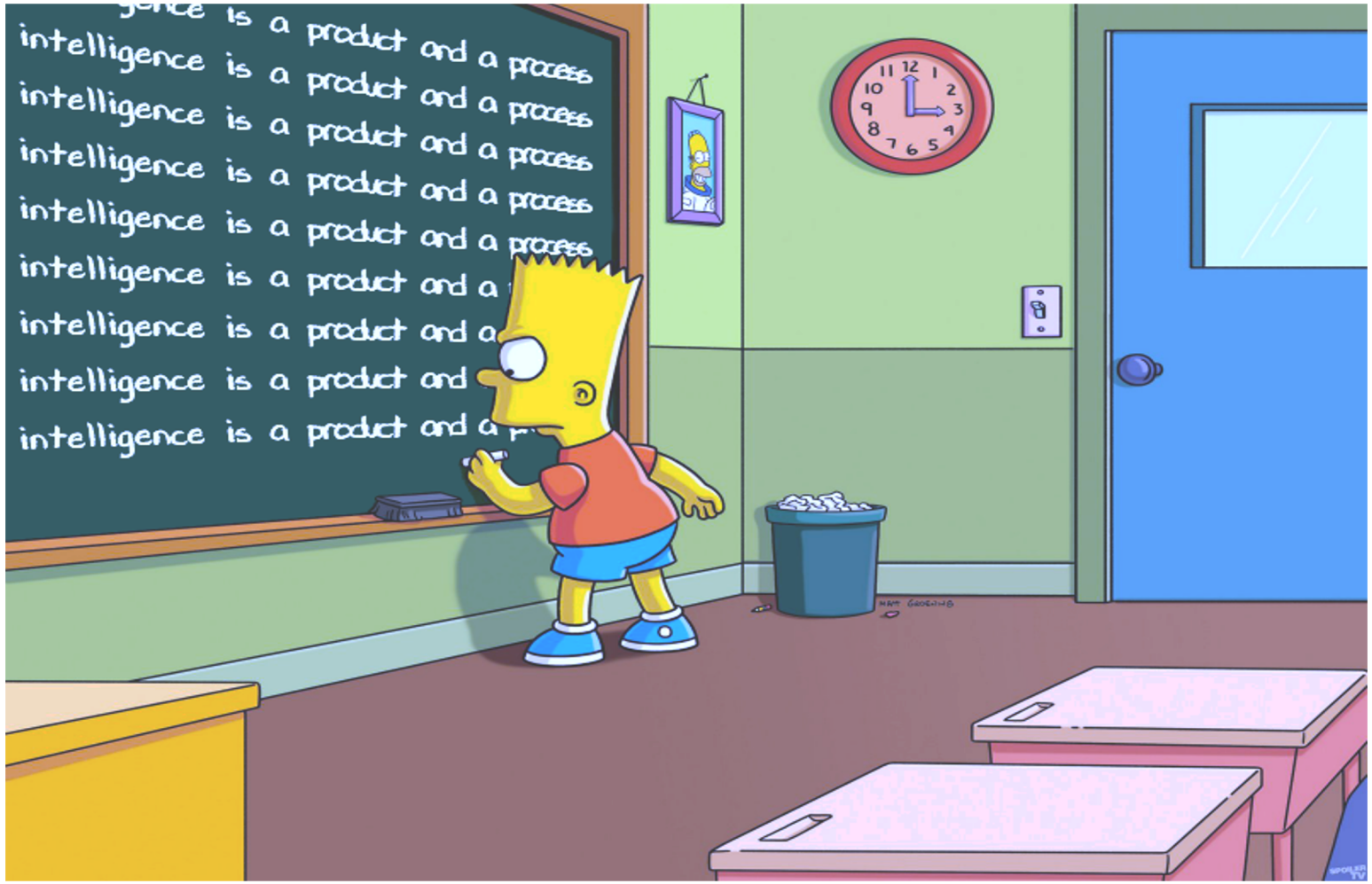
- SANS CTI Surveys
- Rick Holland - Threat Intelligence Awakens, Threat Intelligence Is Like Three Day Potty Training
- S. Brown, J. Gommers and O. Serrano - From Cyber Security Information Sharing to Threat Management
- Scott J Roberts - Community Intelligence & Open Source Tools: Building an Actionable Pipeline
- FireEye - Excelerating Analysis

Resources for this presentation: https://bit.ly/ctisummit2021

The current state of TIPs

(Present)

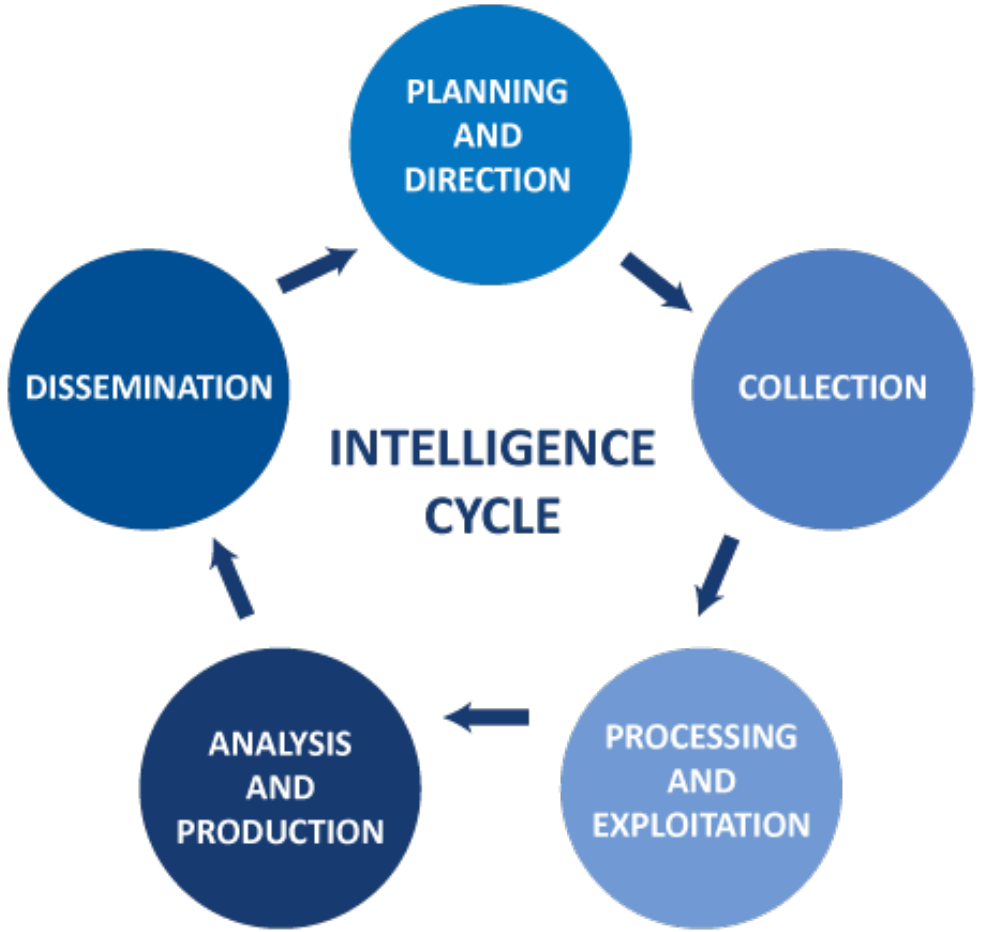
CTI 101


intelligence is a product and a process
intelligence is a product and a process
intelligence is a product and a process
intelligence is a product and a process
intelligence is a product and a process
intelligence is a product and a
intelligence is a product and a
intelligence is a product and
intelligence is a product and a

Please welcome the intelligence cycle

”Your intelligence program’s maturity is based on your ability to do each part of the intelligence cycle”

Reference: Intel471



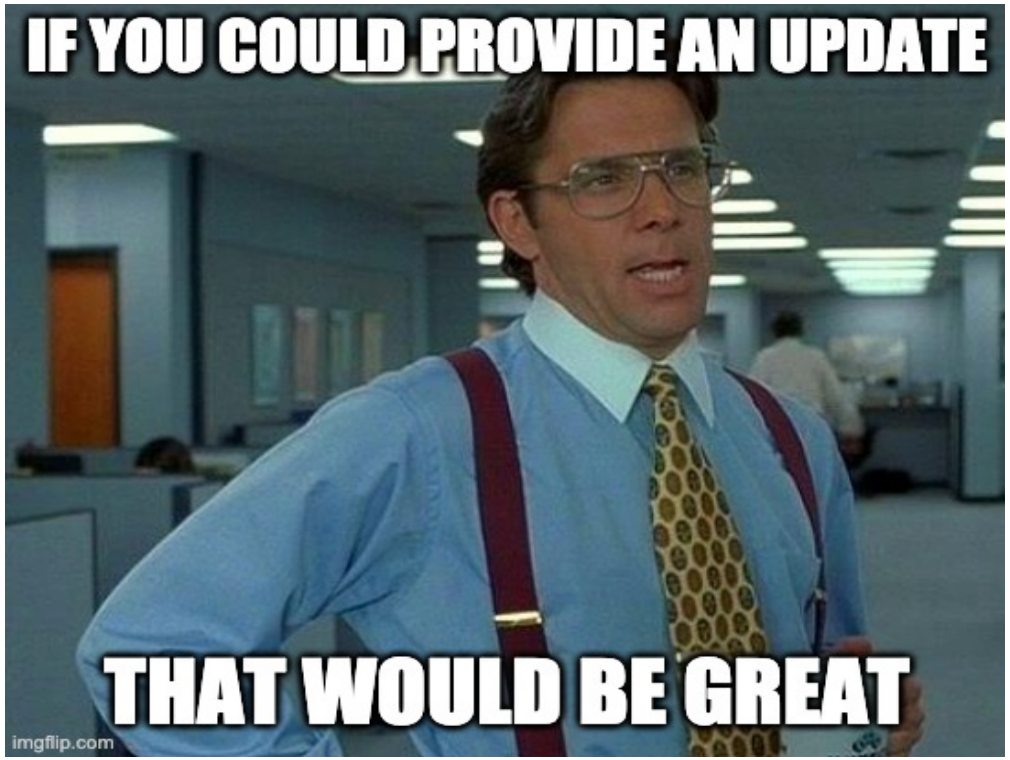
Exceling at TIP requirements

Annex B: Detailed TIP functional requirements

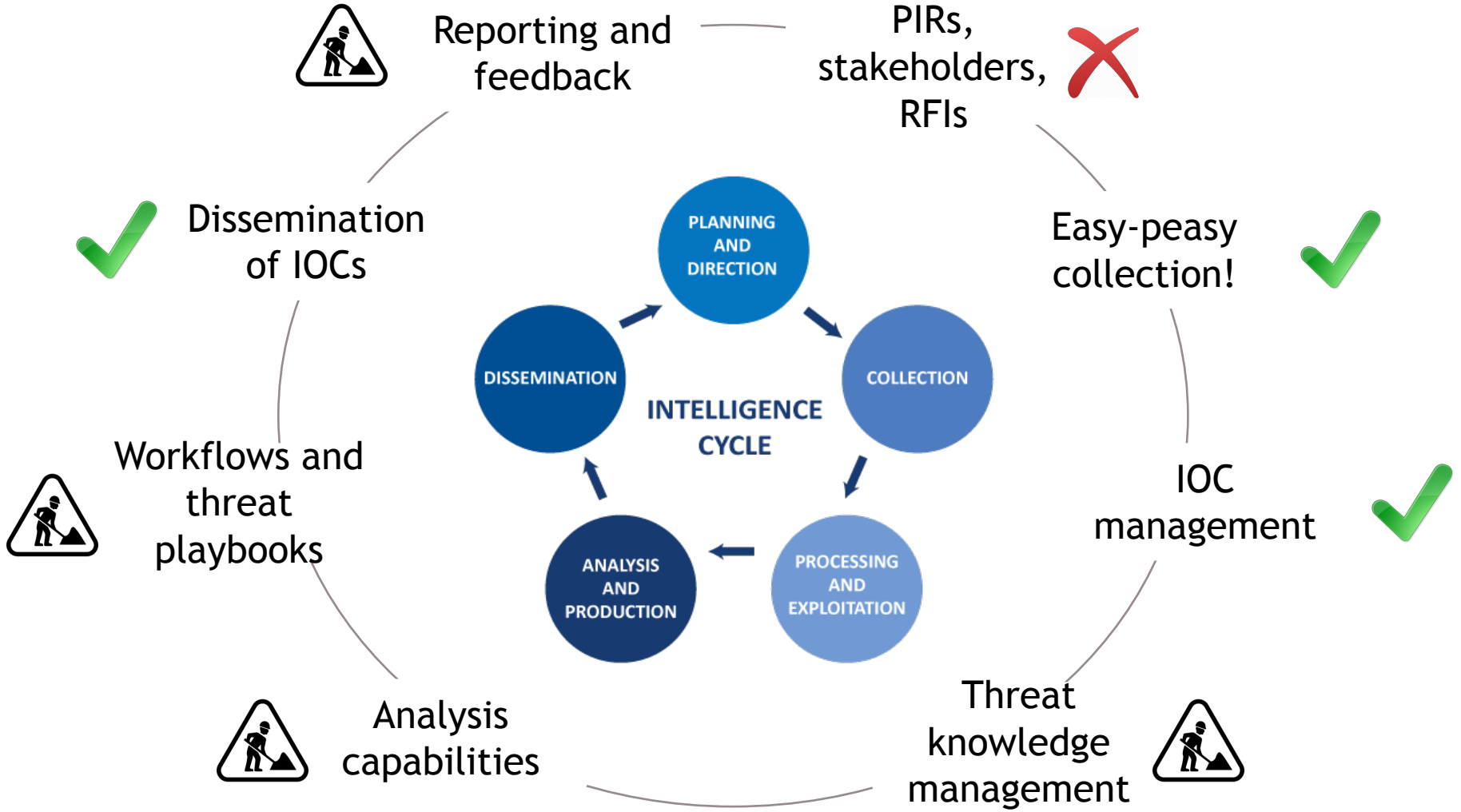
Excel sheet for TIP functional requirements can be found in GitHub link below

Resources for this presentation: https://bit.ly/ctisummit2021

But what about the current state of TIPs?



Let’s walk again the intelligence cycle



Recap
The current state of TIPs

- Focus on collection, IOC management, normalisation, and IOC dissemination
- Transitioning from IOC management to threat knowledge management
- Limited support for intelligence lifecycle end to end

CURRENT STATUS

MAKING PROGRESS
BUT STILL A LONG WAY TO GO

Resources
The current state of TIPs

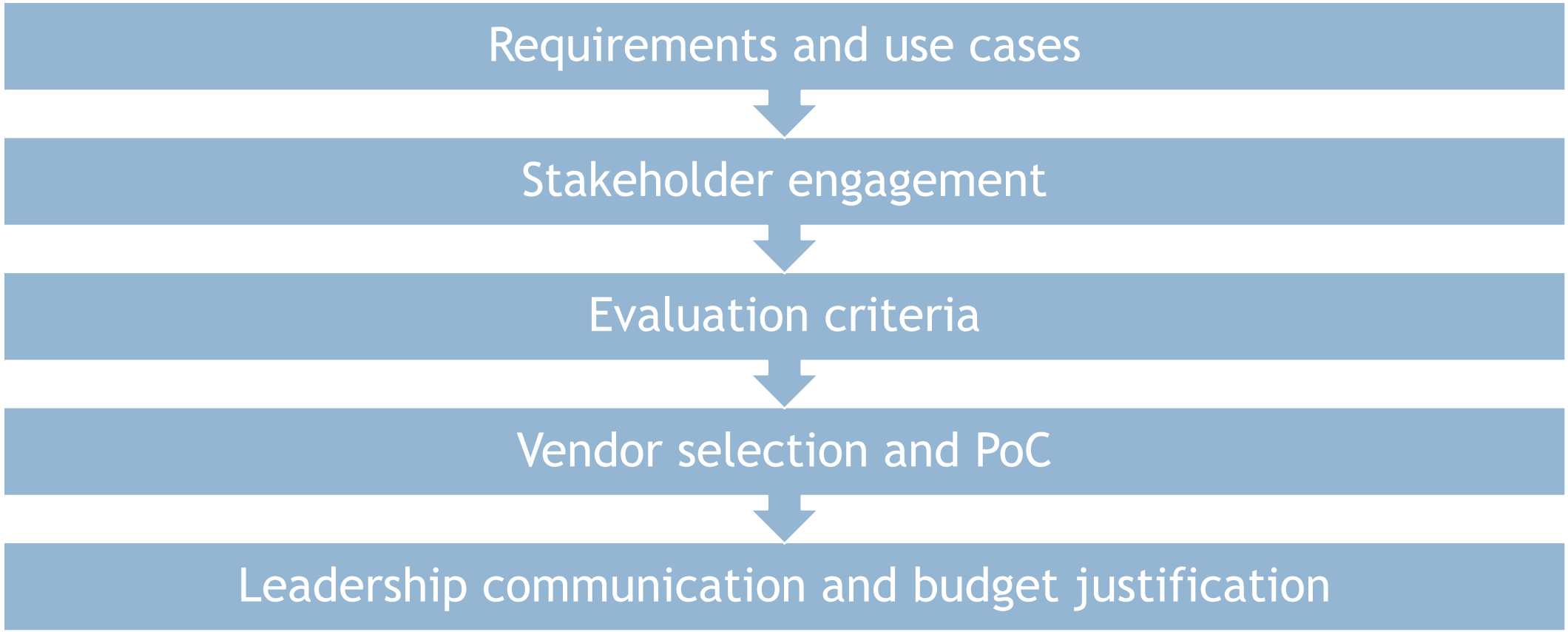
- ENISA - Exploring the opportunities and limitations of current Threat Intelligence Platforms
- Andy Piazza - An Analyst's Need for a Threat Intelligence Platform
- SEI Carnegie Mellon University - Cyber Intelligence Tradecraft Report
- C. Sauerwein, C. Sillaber, A. Mussmann and R. Breu - Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives
- threatintel.eu - Exceling at Threat Intelligence Platform (TIP) requirements

Resources for this presentation: https://bit.ly/ctisummit2021

Looking ahead

(Future)

What's the best TIP for my org?



Reference:
Jason Wonn / Andy Piazza

Best practices for CTI teams

Requirements

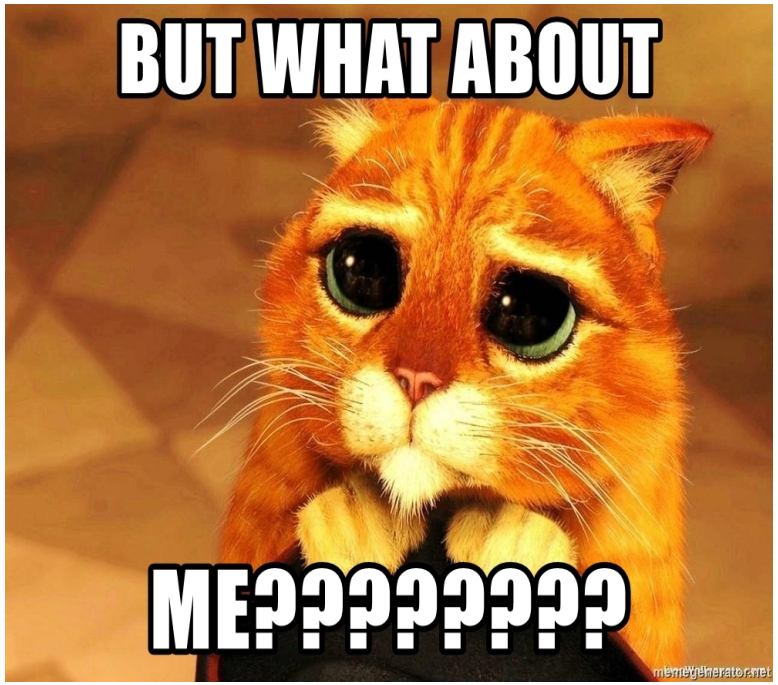
Style Guide

SOPs and Playbooks

Feedback

Recommendations for TIP vendors and developers

- Current state of the TIP landscape
- Strive for feedback
- CTI analyst focused
- Educate your customers/end users
- Communicate your roadmap



The Future of TIPs

Recap
Looking ahead

- Best practices for selecting and using TIPs
- Recommendations for TIP vendors and developers
- The future of TIPs

Reference: Andy Piazza

Resources
Looking ahead

- BSidesNOVA - Jason Wonn - TIP of the Spear: A Threat Intelligence Platform Acquisition
- Andy Piazza - An Analyst's Need for a Threat Intelligence Platform
- FIRST CTI 2019 – Pasquale Stirparo – Your requirements are not my requirements
- Frost & Sullivan - Assessment of the Global Threat Intelligence Platforms Market, Forecast to 2022
- ENISA - Exploring the opportunities and limitations of current Threat Intelligence Platforms

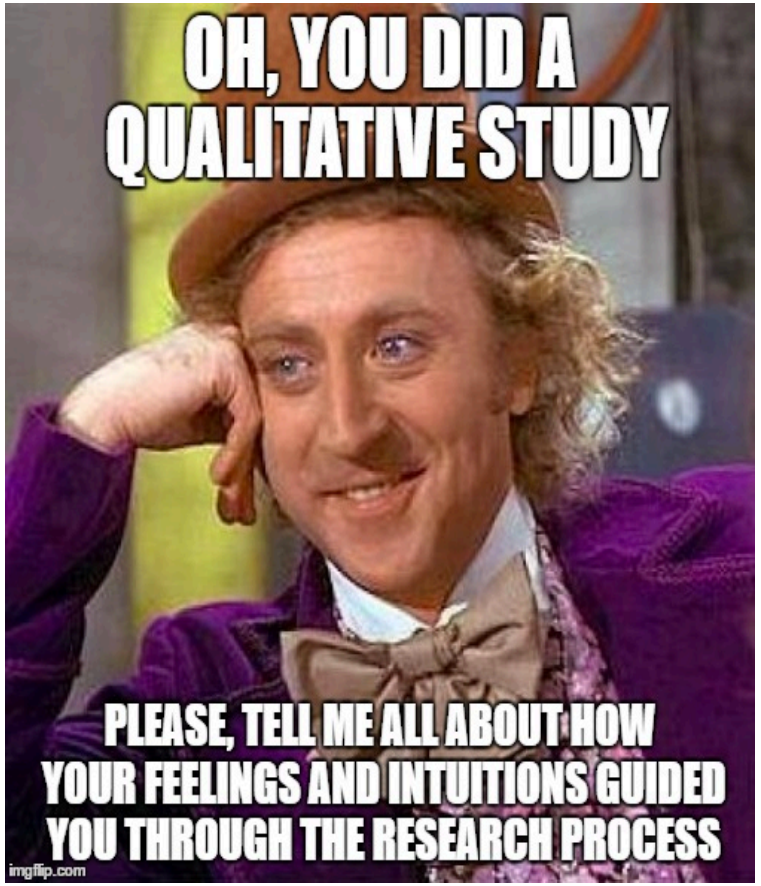
Resources for this presentation: https://bit.ly/ctisummit2021

Final Remarks

Final Remarks

- Support CTI with a variety of integrated tools
- Follow best practices for selecting and using your TIP
- It takes two to tango… and further mature

Thanksgiving slide



Thanksgiving slide

CTI PROS

Razvan Gavrila

Chris Beard

Sarah Brown

Alexandre Dulaunoy

Jane Ginn

Pasquale Stirparo

Omid Raghimi

Jason Wonn

Andy Piazza

Derek Buchanan

Samantha Loh

Megan Kaczanowski

Pierre Lamy

TIP VENDORS

D3 Intelligence - Brian Mohr

QuoLab Technologies - Fabien Dombard

TruSTAR - Shimon Modi

Analyst1 – P. Terry, C. Hoffman, J. Nixon

Anomali – Frank Lange

ThreatConnect – Andrew Pendergast

EclecticIQ - Aukjan van Belkum, Mark Huijnen

IntSights - Yuval Inchi

LookingGlass - Allan Thomson

MARKET RESEARCH

Forrester - Brian Kime

Thank you!

Andreas Sfakianakis

@asfakian

Resources for this presentation: https://bit.ly/ctisummit2021

tilting at windmills

threatintel.eu