

5 YEARS OF APPLIED CTI DISCIPLINE

WHERE SHOULD ORGANISATIONS PUT FOCUS ON?

FIRST CTI 2019

Andreas Sfakianakis

CTI Professional



WHO AM I

- CTI and IR professional in Financial and Oil & Gas sectors
- Member of ENISA CTI Stakeholder Group
- External Expert for ENISA and European Commission
- Twitter handle: @asfakian / Website: www.threatintel.eu

tilting at windmills

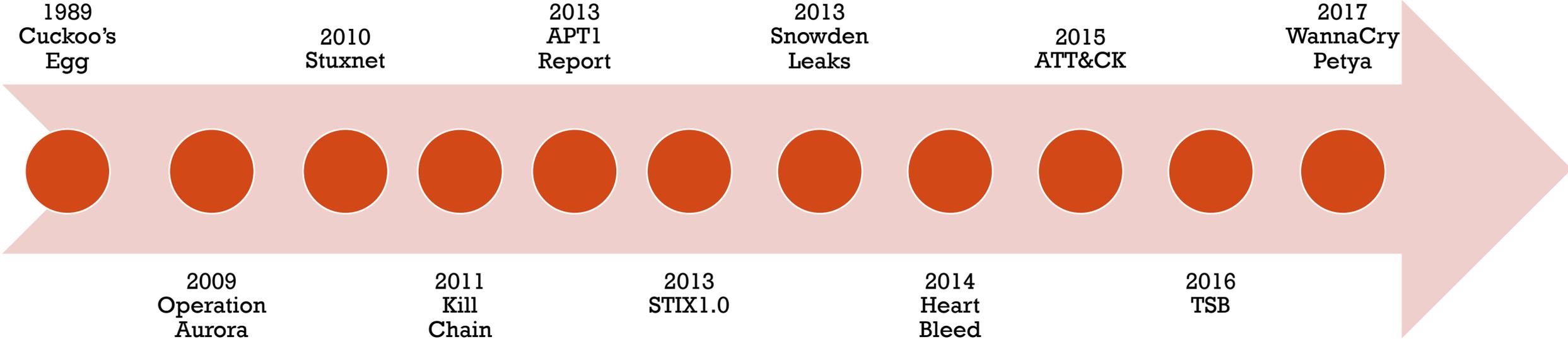


DISCLAIMER

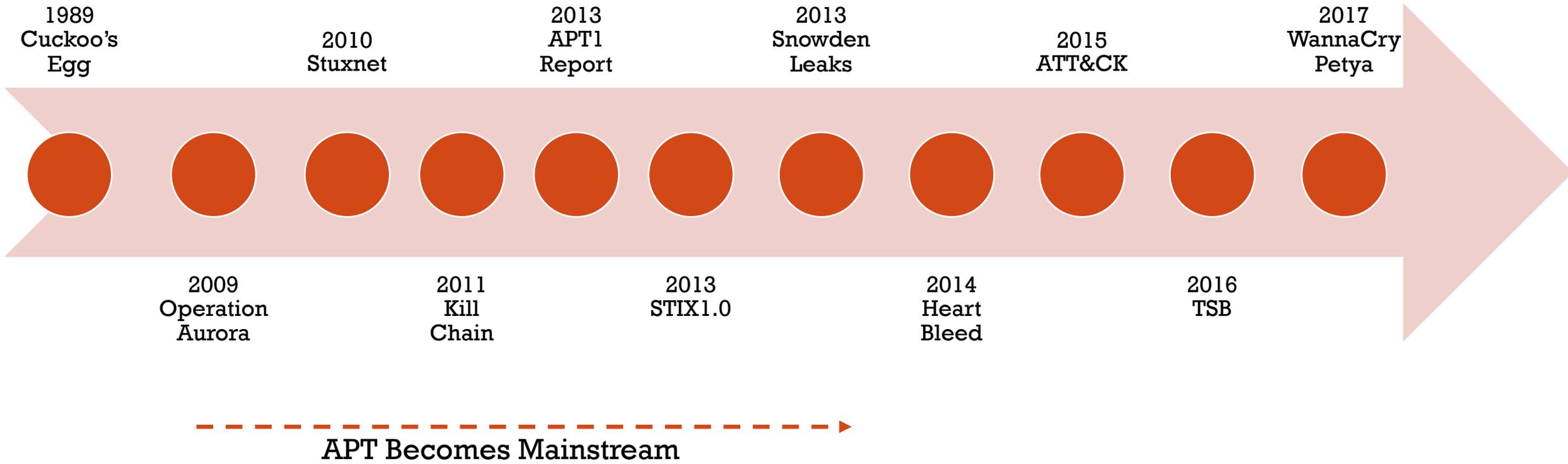
- Original authors are **referenced** within the slide deck.
- References for this presentation <http://bit.ly/first-cti-2019>
- Views are my own and not my employer's



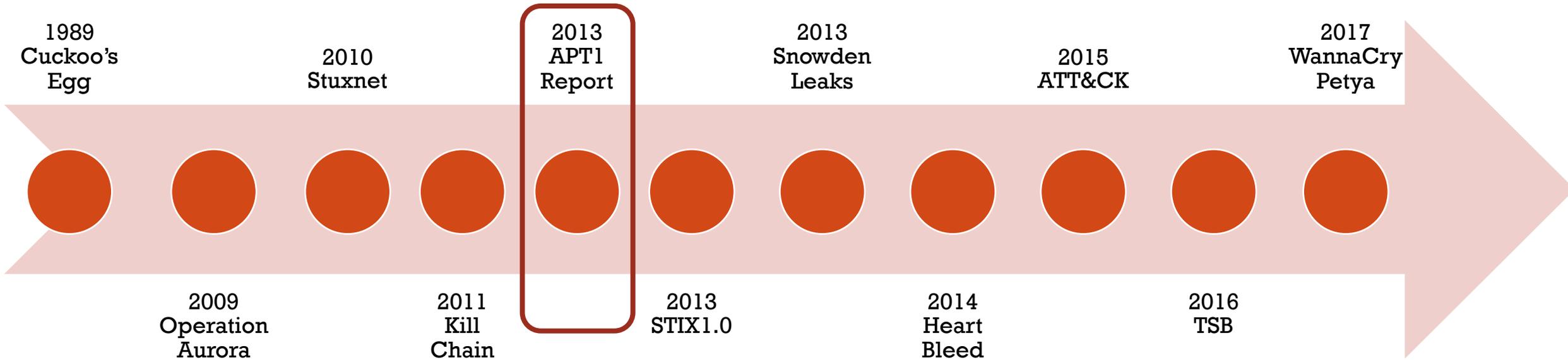
TIMELINE OF IMPORTANT EVENTS IN CTI



TIMELINE OF IMPORTANT EVENTS IN CTI



TIMELINE OF IMPORTANT EVENTS IN CTI

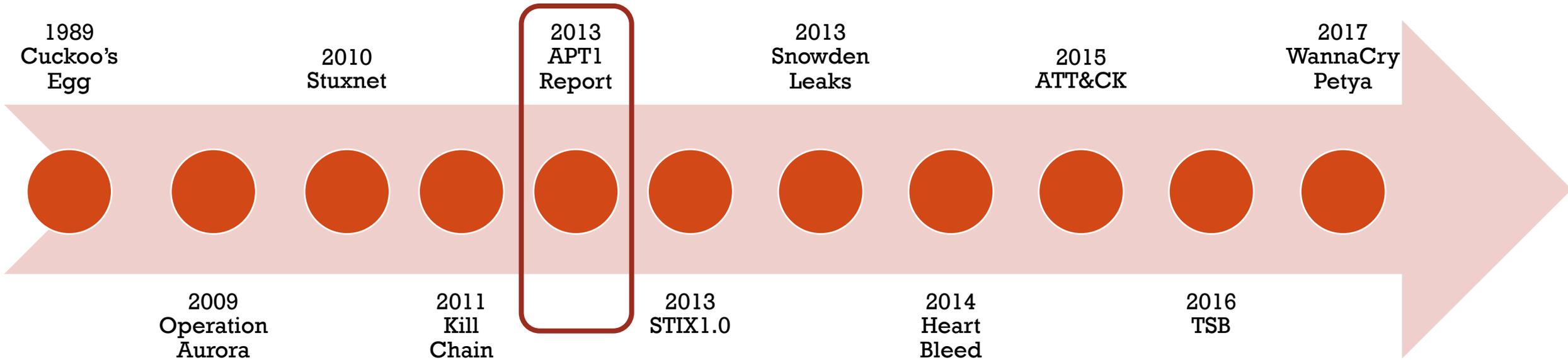


APT Becomes Mainstream



TIMELINE OF IMPORTANT EVENTS IN CTI

CTI Adoption



APT Becomes Mainstream



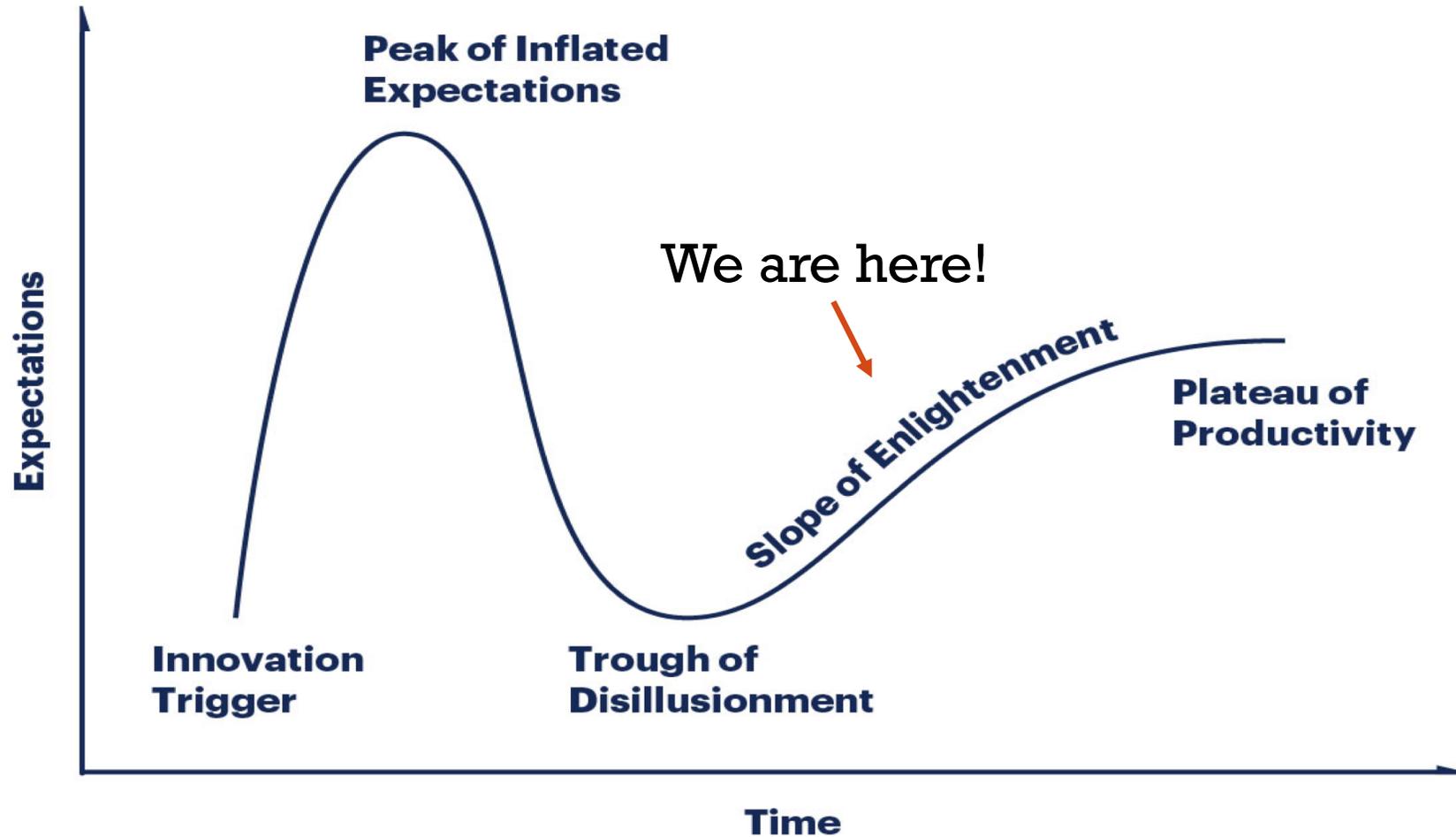
AS A COMMUNITY, WE DID GREAT PROGRESS!

	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:



CTI HYPE CYCLE



Reference:

Gartner



**WHAT ARE THE AREAS THAT
CTI TEAMS COULD HAVE PERFORMED
BETTER DURING THE LAST 5 YEARS?**

Problem Statement



#1 INTELLIGENCE DIRECTION

- 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 Controls

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



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

Following



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

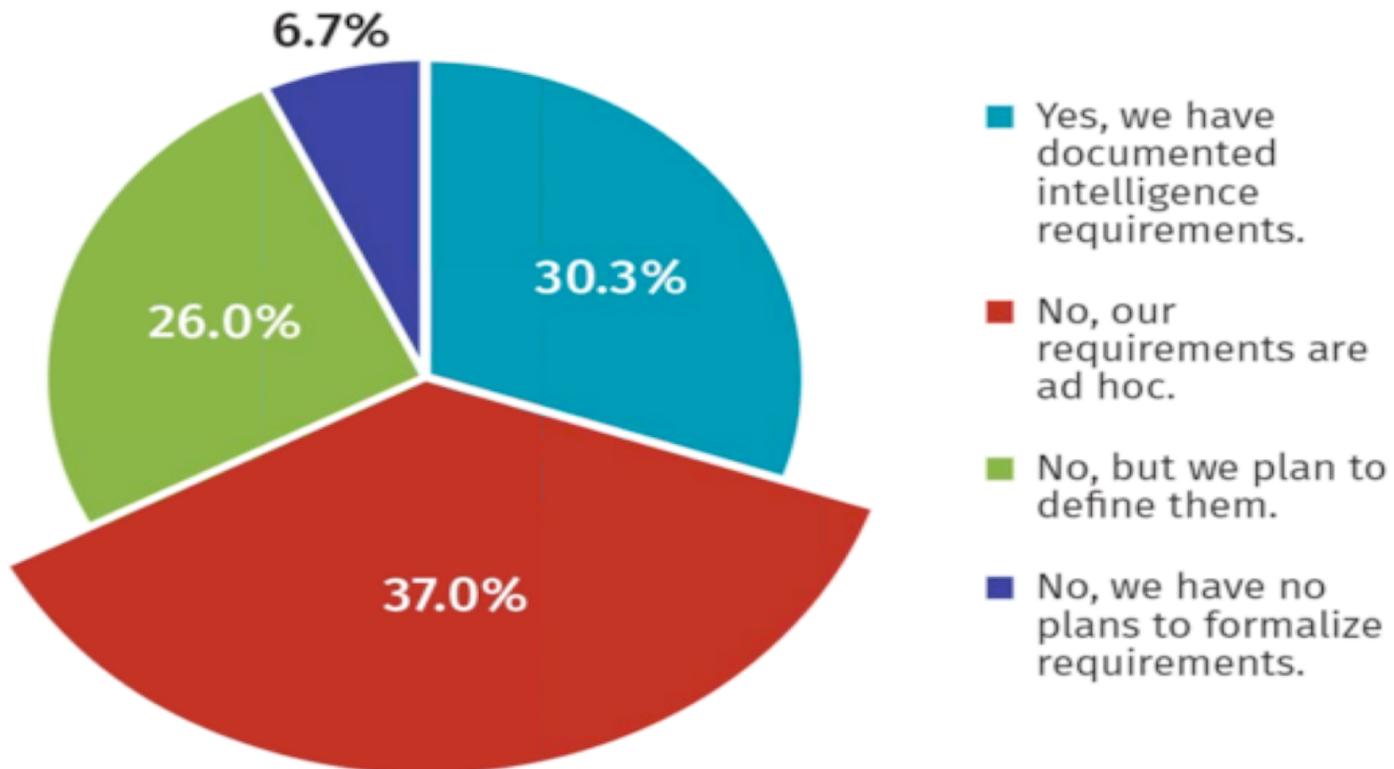
6:23 PM - 15 Aug 2016

Reference:
Sergio Caltagirone



DOCUMENTED INTELLIGENCE REQUIREMENTS?

Are CTI requirements clearly defined in your organization?



Reference:
SANS



RESOURCES — INTELLIGENCE DIRECTION

- 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



RECAP – INTELLIGENCE DIRECTION

- Identification of relevant stakeholders
- Connection with business and enterprise risk management cycles
- Better/accurate identification of operational environment (crown jewels)
- Capturing and documenting the intelligence requirements

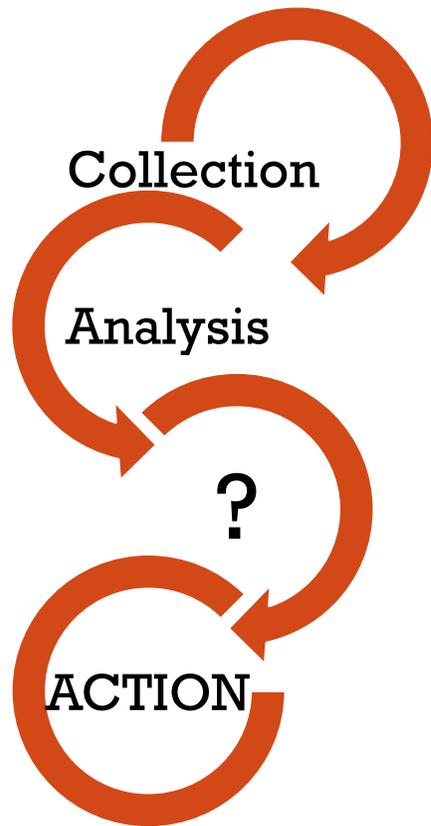


#2 FINALIZED REPORT AND DISSEMINATION

- Value of finalized reporting
- Embedding of intelligence tradecraft (cross-pollination)
- Means of dissemination

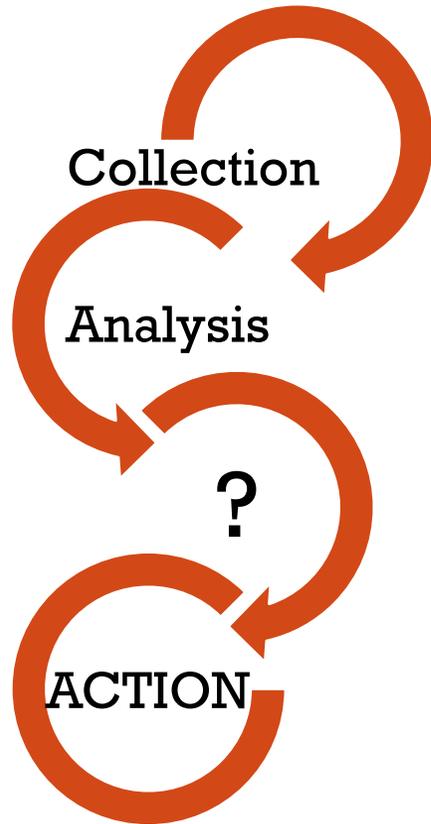


FINALIZED INTELLIGENCE PRODUCT

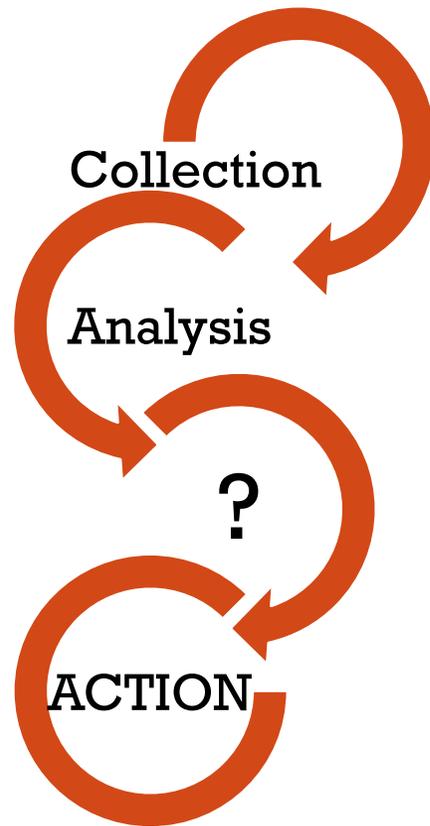


FINALIZED INTELLIGENCE PRODUCT

- Intelligence and production requirements



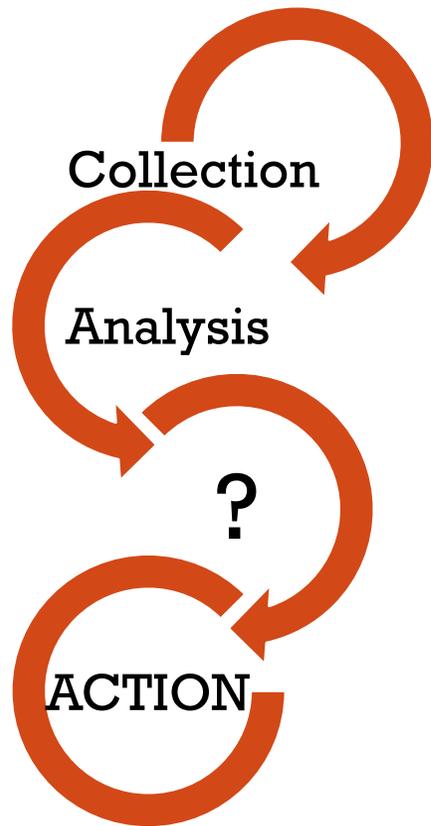
FINALIZED INTELLIGENCE PRODUCT



- Intelligence and production requirements
- Structure - Report template



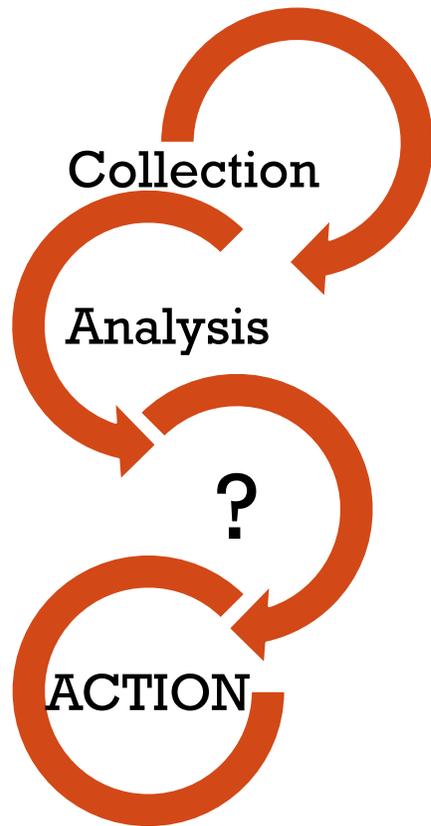
FINALIZED INTELLIGENCE PRODUCT



- Intelligence and production requirements
- Structure - Report template
- Style - Style guide document



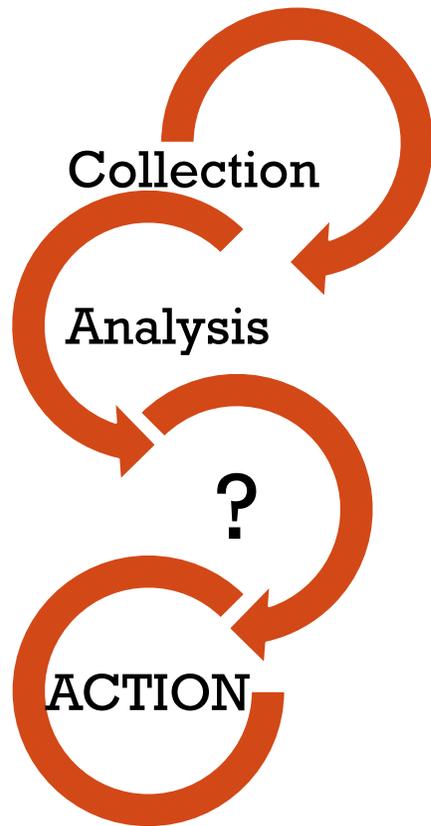
FINALIZED INTELLIGENCE PRODUCT



- Intelligence and production requirements
- Structure - Report template
- Style - Style guide document
- Tradecraft –
IC Analytic Standards (ICD 203)
/ DI Quality Framework



FINALIZED INTELLIGENCE PRODUCT



- Intelligence and production requirements
- Structure - Report template
- Style - Style guide document
- Tradecraft –
IC Analytic Standards (ICD 203)
/ DI Quality Framework
- Constant feedback loop



SUCCESS STORIES - REPORTING

Report Structure

- Executive Summary (BLUF)
- What?
- So what?
- So what of the so what? What next?
- References
- Appendix
 - Indicators
 - Tradecraft used



SUCCESS STORIES - DISSEMINATION

- Internal Communications / Email marketing application to capture feedback
- Brand your intel products
- Nice design & layout
- Mobile friendly
- Capture statistics
- Indirect extraction of requirements



The Importance of
Tracking Internal Email
Communications

HOW ORGANIZATIONS BENEFIT FROM EMAIL ANALYTICS



SUCCESS STORIES - DISSEMINATION

- Store the intel products in SharePoint
- Access control & Confidential reports
- Capture Site stats
- Measure outreach



The screenshot displays a SharePoint site dashboard with the following components:

- Navigation:** Home, Notebook, Documents, Big Wins, Site Contents (selected), Recycle bin, Contoso Operations.
- Site visits:** 42 views in the last 7 days, +15% over the previous week.
- Trending content:**
 - Contract Proposals.docx (25 views)
 - Northwind presentation.pptx (19 views)
 - Contoso Product Innovation.pdf (12 views)
 - All Japan Revenues By City.xlsx (7 views)
- Tips:** Make it your own - Customize your homepage and highlight content and data using web parts.
- Contents Table:**

Name	Type	Items	Modified
Documents	Document library	2	7 days ago
Site Assets	Document library	2	10 days ago
Big Wins	List	19	9 days ago
Engine Parts	List	0	9 days ago
Garthf Wins	List	6	9 days ago
MicroFeed	List	2	4/8/2016
Site Pages	Wiki page library	2	9 days ago



JOURNALISM & CTI



Following



A lot of journalists have been laid off. If your threat intelligence team is hiring you should encourage journalists to apply. Excellent technical writers that work under pressure with short deadlines; technical writers are a staple of good threat intel teams.

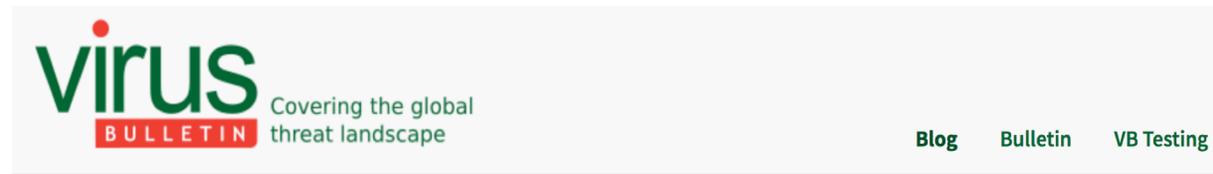
5:22 PM - 25 Jan 2019

86 Retweets 256 Likes



8 86 256

Reference:
Robert M. Lee



Threat intelligence teams should consider recruiting journalists

Posted by  Martijn Grooten on Jan 29, 2019

Reference:
VB – Martijn Grooten



RELEVANT TRAININGS

- Chris Sander's Effective Information Security Writing
- SANS SEC402: The Secrets to Successful Cybersecurity Writing: Hack the Reader
- Write it or didn't happen 😊



RESOURCES - INTELLIGENCE REPORTING

- Intelligence Community Directive (ICD) 203 - Analytic Standards
- CIA - Analytic Thinking and Presenting for Intelligence Producers
- CIA - Compendium of Analytic Tradecraft Notes
- CIA - Style Manual and Writers' Guide for Intelligence Publications
- The Economist Style Guide
- SANS CTI Summit 2017 - Pen-To-Paper and The Finished Report: The Key To Generating Threat Intelligence - Christian Paredes
- SANS CTI Summit 2019 - Analytic Tradecraft in the Real World - Amy R. Bejtlich
- Sergio Caltagirone - 15 Things Wrong with Today's Threat Intelligence Reporting
- Lenny Zeltser - Top 10 Writing Mistakes in Cybersecurity and How You Can Avoid Them



RECAP - INTELLIGENCE REPORTING

- CTI needs to be better communicated to business at a strategic (and operational) level.
- Communication competencies are key for CTI teams.
 - Report writing as a critical CTI skill.
- Cross-pollination - Intelligence tradecraft wasn't invented yesterday



#3 CTI ANALYST SKILLSET

- CTI skills shortage
 - *SANS CTI Survey 2018: “62% of respondents cited a lack of trained CTI professionals and skills as a major roadblock, an increase of nearly **10 percentage points over 2017 (53%)**”*
- Organizational challenges
- Challenges for CTI teams



CHALLENGES FOR CTI TEAMS

- What is the skillset needed for a CTI team?
 - *“Do I need a reverse engineer for my CTI team?”*
 - *“Do I need non-technical analysts in my team?”*
- How we develop the skillset of (junior) CTI analysts?
- How do we streamline day to day CTI work?
 - *“How do I reduce CTI analyst dependency?”*



CTI ANALYST COMPETENCIES

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:



CTI ANALYST COMPETENCIES

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.

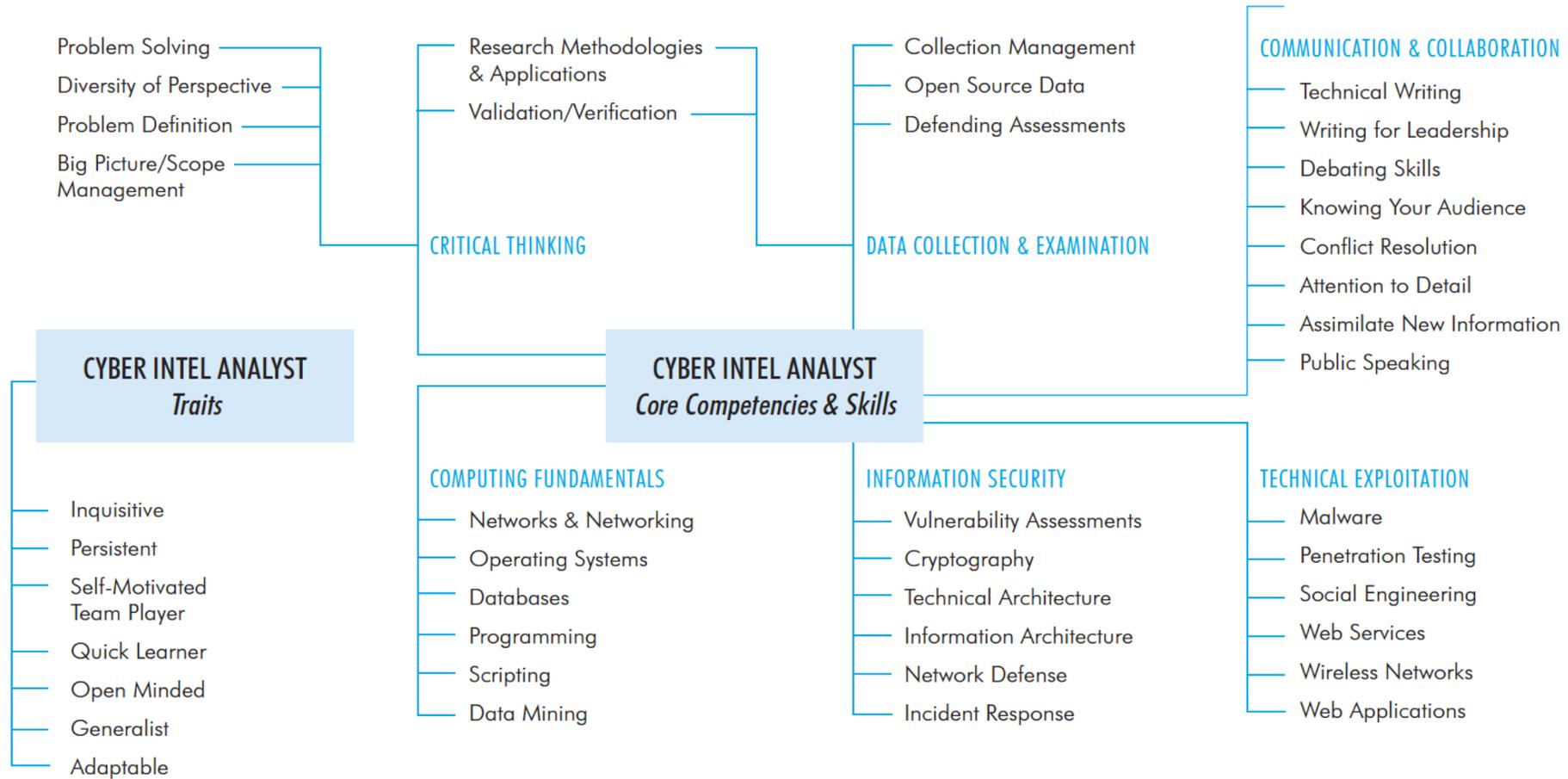
CONTEXTUAL DOMAIN COMPETENCIES

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:



CTI ANALYST COMPETENCIES



Reference:



DEVELOPING CTI SKILLS AND STREAMLINING CTI OPERATIONS

- Core CTI curriculum and CTI training roadmap
- Documented Standard Operating Procedures (SOPs)
- Review process as a learning opportunity
- Periodic exercises with your team (SATs or intrusion analysis)
 - Knowing your biases?



RESOURCES — CTI ANALYST SKILLSET

- INSA - Cyber Intelligence: Preparing Today's Talent for Tomorrow's Threats
- Sergio Caltagirone - 15 Knowledge Areas and Skills for Cyber Analysts and Operators
- EclecticIQ – On the Importance of Standard Operating Procedures in Threat Intelligence
- CIA - Making the Analytic Review Process Work
- CIA – Fifteen Axioms for Intelligence Analysis
- ENISA CTI-EU 2017 - Lessons Learned from Teaching CTI All Over the World - Jess Garcia
- ComradeCookie - What is CTI and what makes a good CTI analyst?
- Richards J. Heuer - Psychology of Intelligence Analysis
- Richards J. Heuer - Structured Analytic Techniques for Intelligence Analysis
- Tali Sharot - The Influential Mind: What the Brain Reveals About Our Power to Change Others



RECAP — CTI ANALYST SKILLSET

- Use a competency based framework to assess your CTI team's skill coverage. CTI skill profile descriptions derived from your requirements.
- Invest on internal/external CTI training opportunities.
- Streamline BAU CTI tasks, make them repeatable.
- Build a working environment for knowledge sharing (sharing is caring, huh?).



FINAL REMARKS

- More focus should be put on implementing key areas of intelligence direction phase.
- CTI reporting and communication can be improved by embedding analytic tradecraft.
- Focus on CTI analyst's skillset.



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

FIRST CTI 2019

Andreas Sfakianakis

CTI Professional

Sharing is caring!

References for this presentation: <http://bit.ly/first-cti-2019>

