5 YEARS OF APPLIED CTI DISCIPLINE

WHERE SHOULD ORGANISATIONS PUT FOCUS ON?

FIRST CTI 2019

Andreas Sfakianakis

CTI Professional

WHO AM I

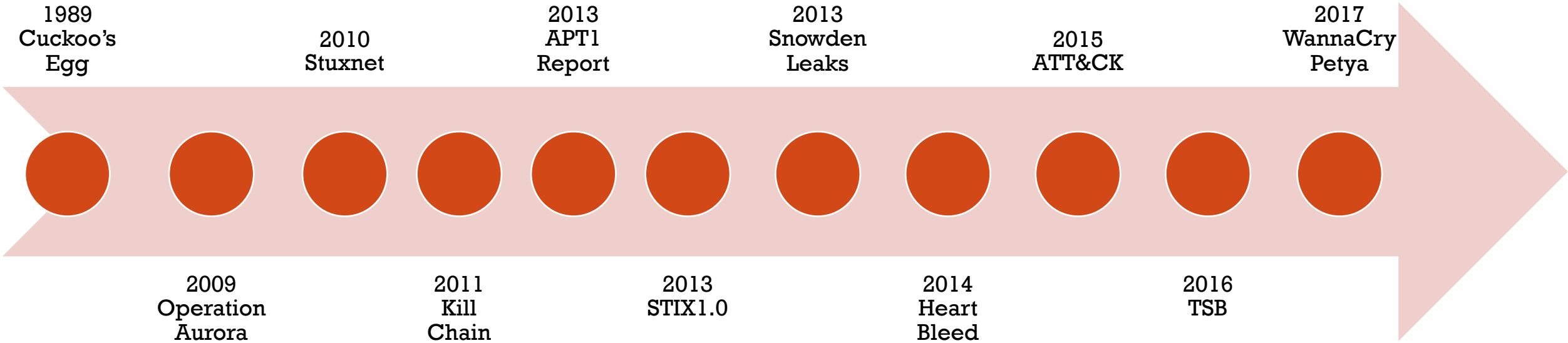
- CTI and IR professional in Financial and Oil & Gas sectors
- Member of ENISA CTI Stakeholder Group
- External Expert for ENISA and European Commission
- Twitter handle: @asfakian / Website: www.threatintel.eu

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

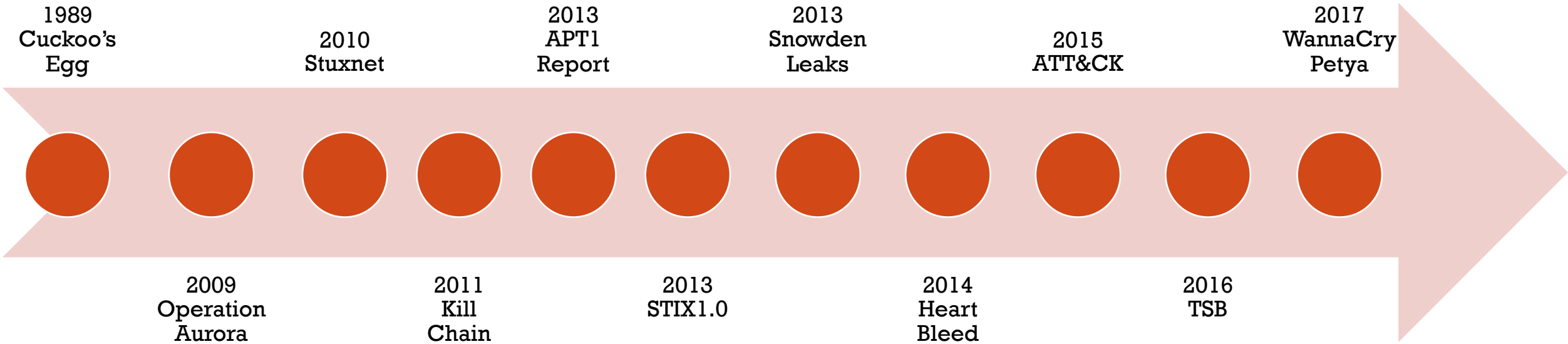
DISCLAIMER

- 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

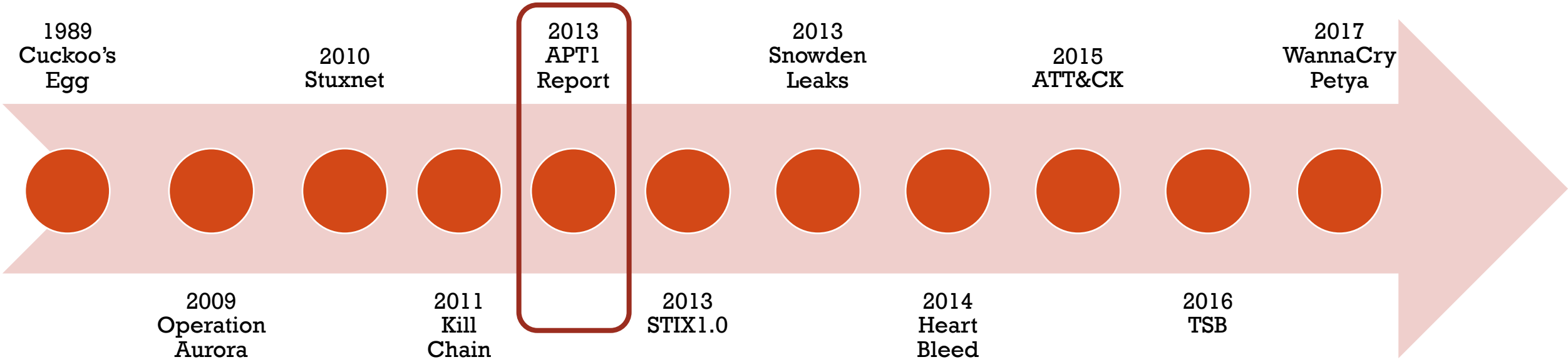


TIMELINE OF IMPORTANT EVENTS IN CTI



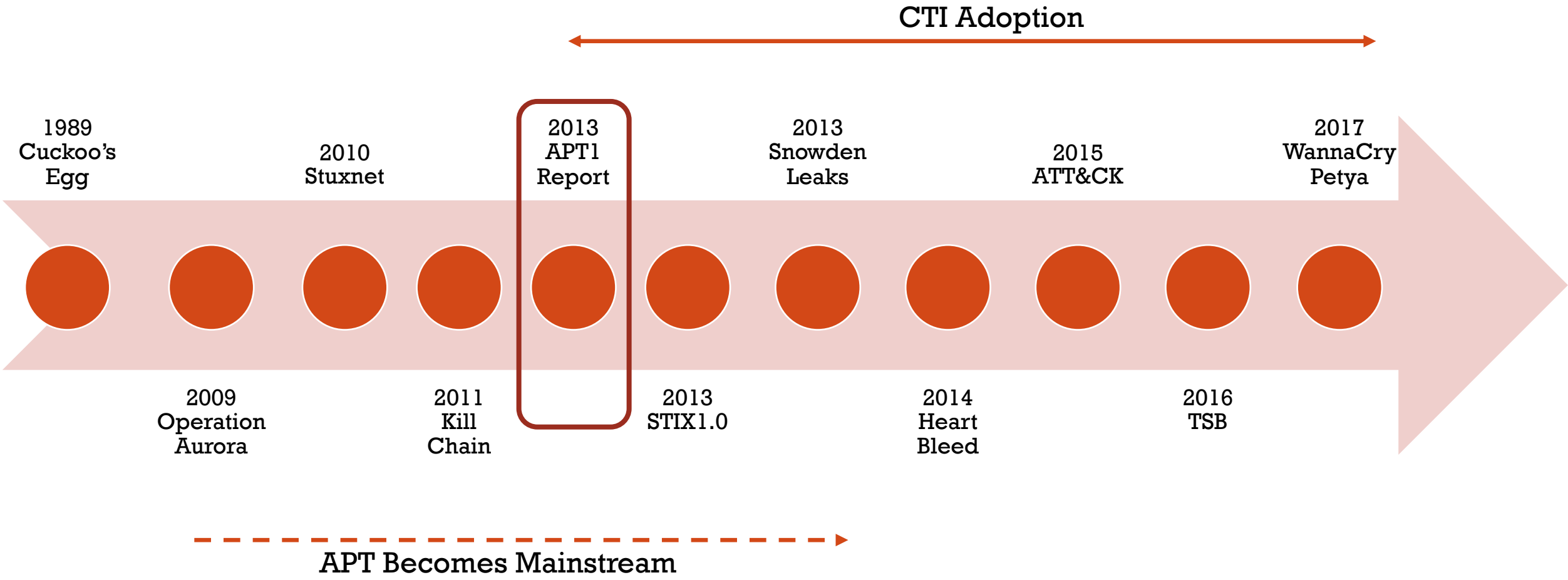
APT Becomes Mainstream

TIMELINE OF IMPORTANT EVENTS IN CTI



APT Becomes Mainstream

TIMELINE OF IMPORTANT EVENTS IN CTI

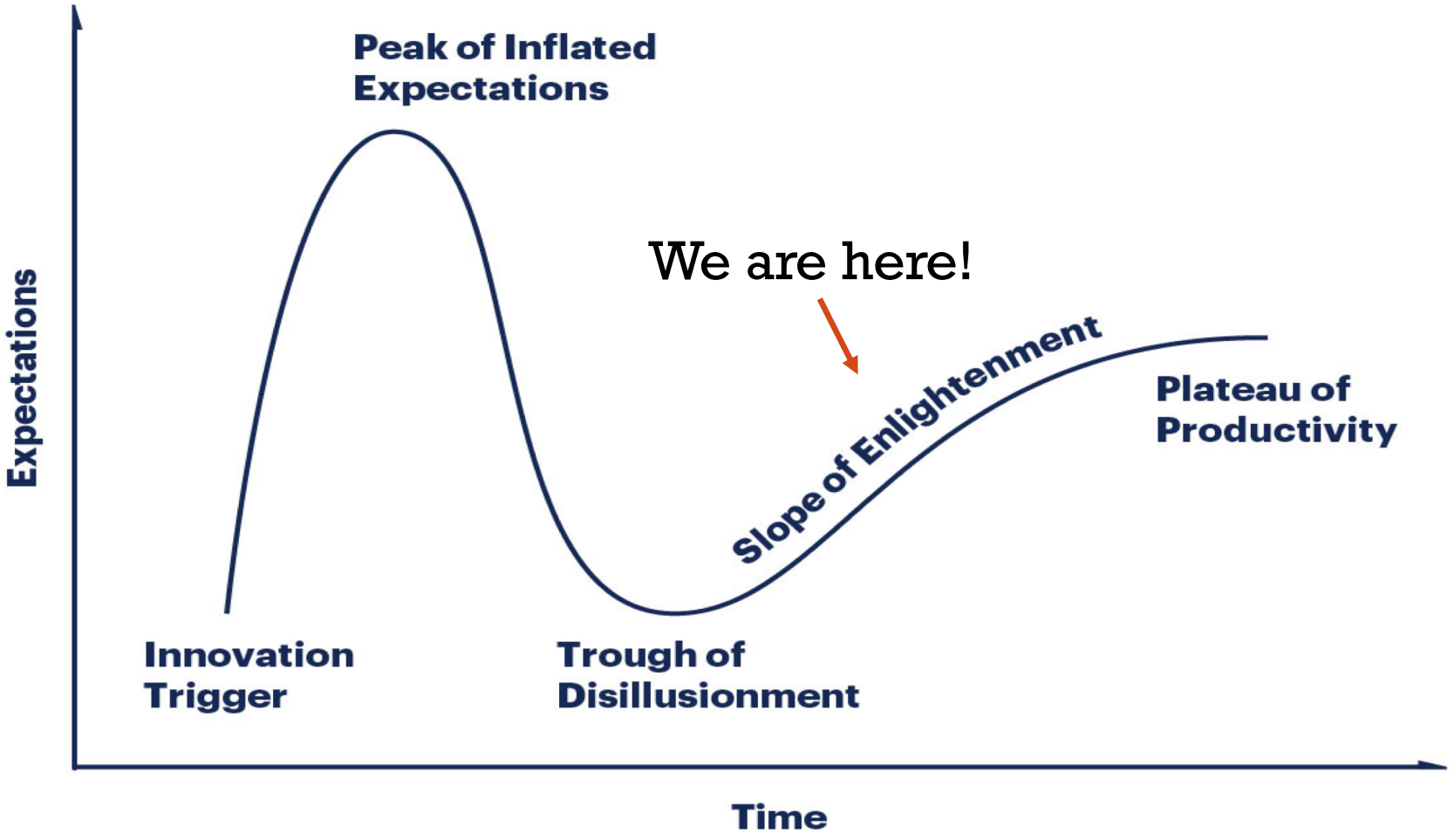


AS A COMMUNITY, WE DID GREAT PROGRESS!

	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 PERMORMED 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

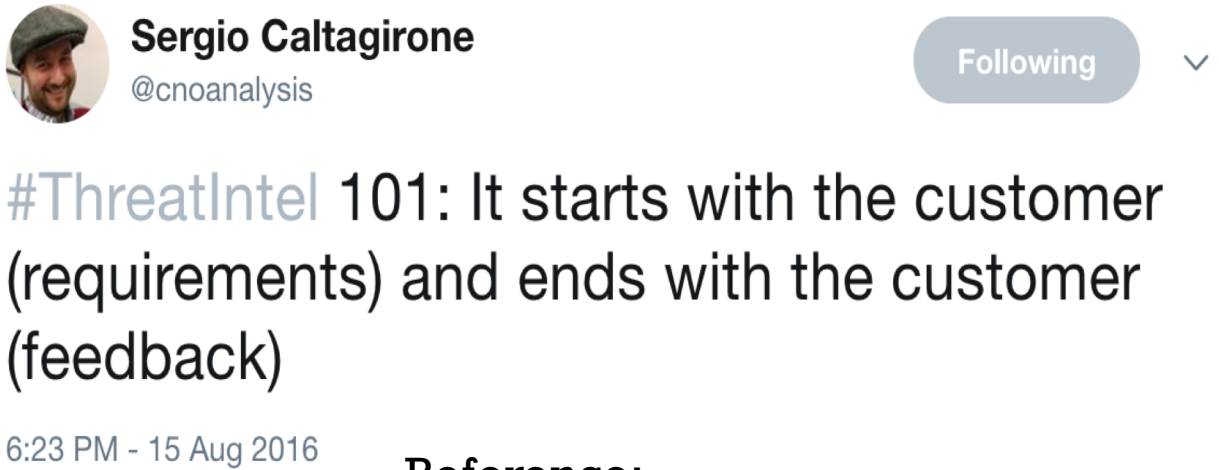
- Incident Responders
- Threat Hunters
- Vulnerability Management
- Red Team
- Fraud Team
- Sys Admins
- IT Managers

Strategic Intelligence

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

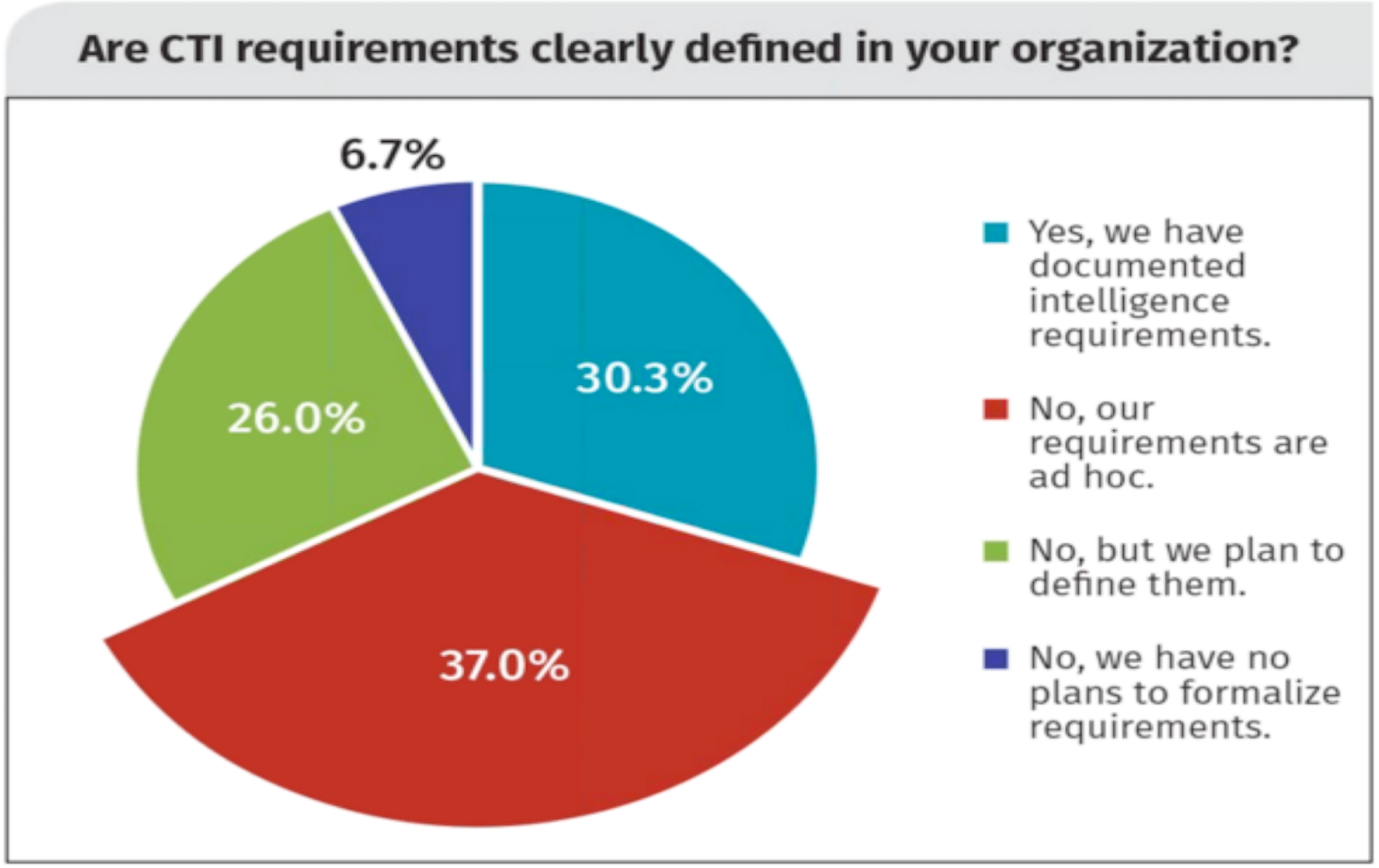
INTELLIGENCE REQUIREMENTS 101

- 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).



Reference:
Sergio Caltagirone

DOCUMENTED INTELLIGENCE REQUIREMENTS?



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

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

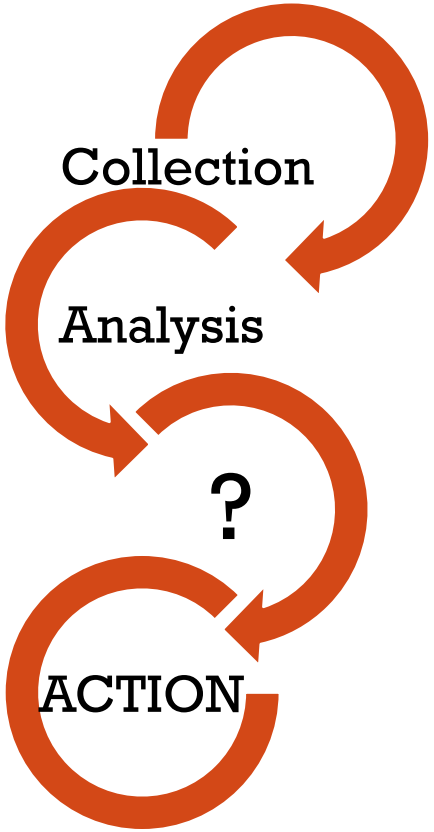
RECAP – INTELLIGENCE DIRECTION

- 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

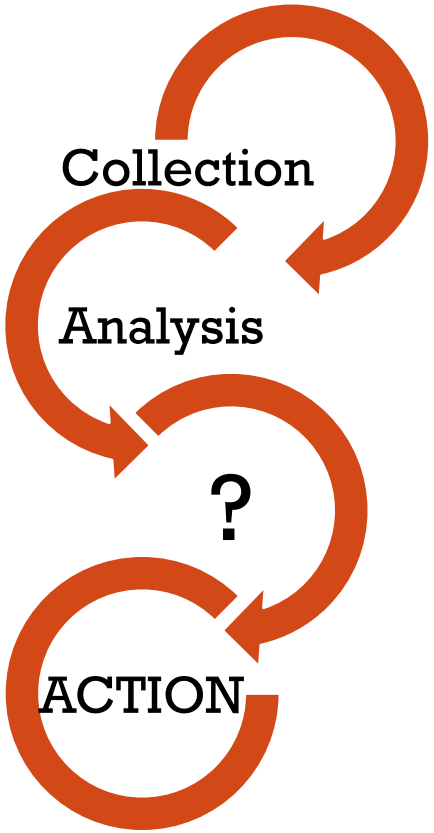
- Value of finalized reporting
- Embedding of intelligence tradecraft (cross-pollination)
- Means of dissemination

FINALIZED INTELLIGENCE PRODUCT



Reference:
Christian Paredes

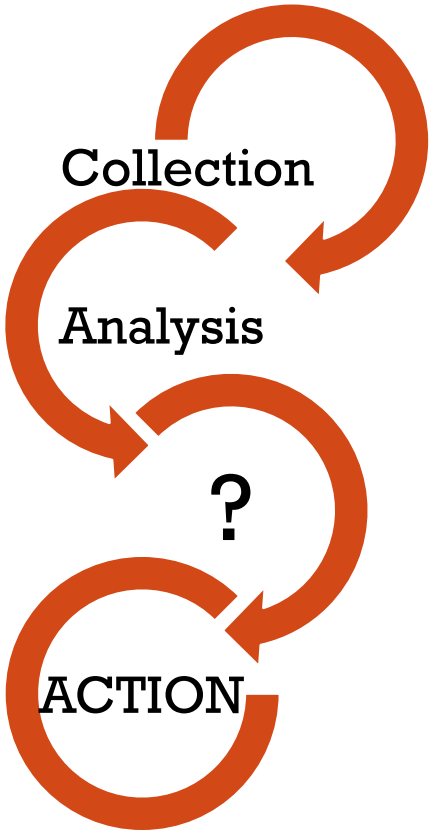
FINALIZED INTELLIGENCE PRODUCT



- Intelligence and production requirements

Reference:
Christian Paredes

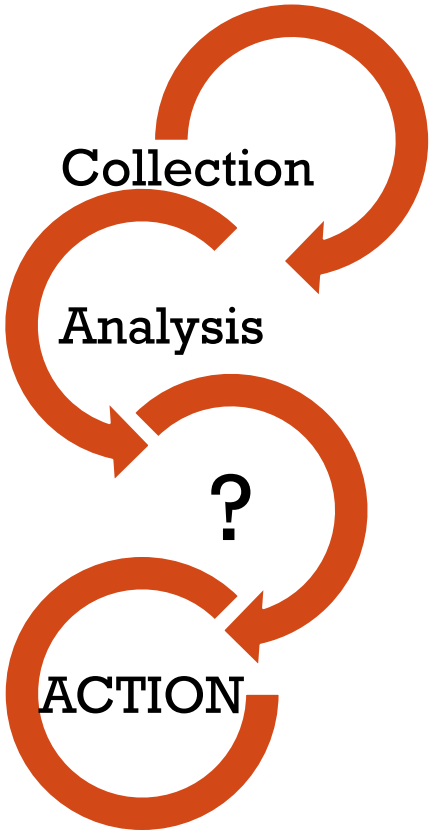
FINALIZED INTELLIGENCE PRODUCT



- Intelligence and production requirements
- Structure - Report template

Reference:
Christian Paredes

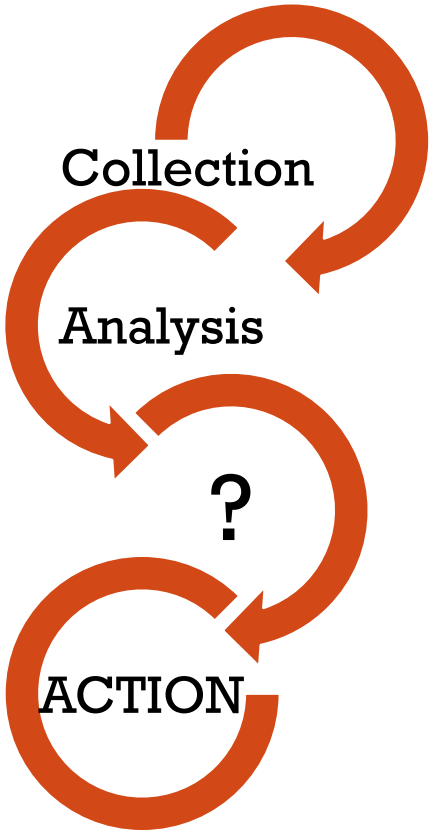
FINALIZED INTELLIGENCE PRODUCT



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

Reference:
Christian Paredes

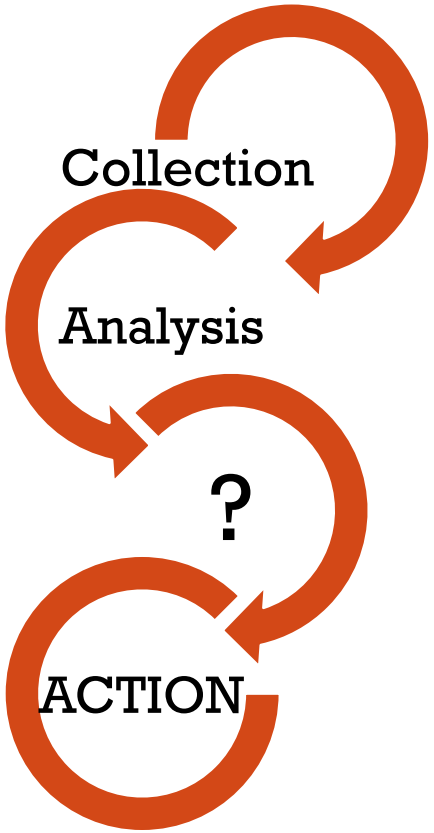
FINALIZED INTELLIGENCE PRODUCT



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

Reference:
Christian Paredes

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

Reference:
Christian Paredes

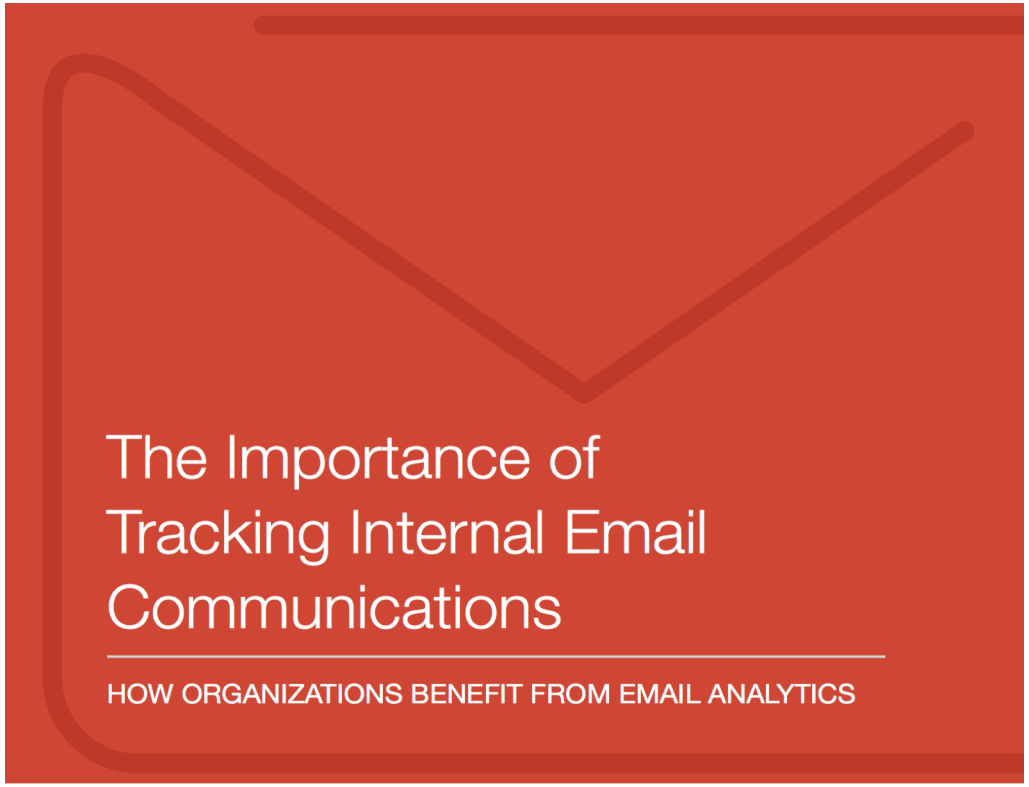
SUCCESS STORIES - REPORTING

Report Structure

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

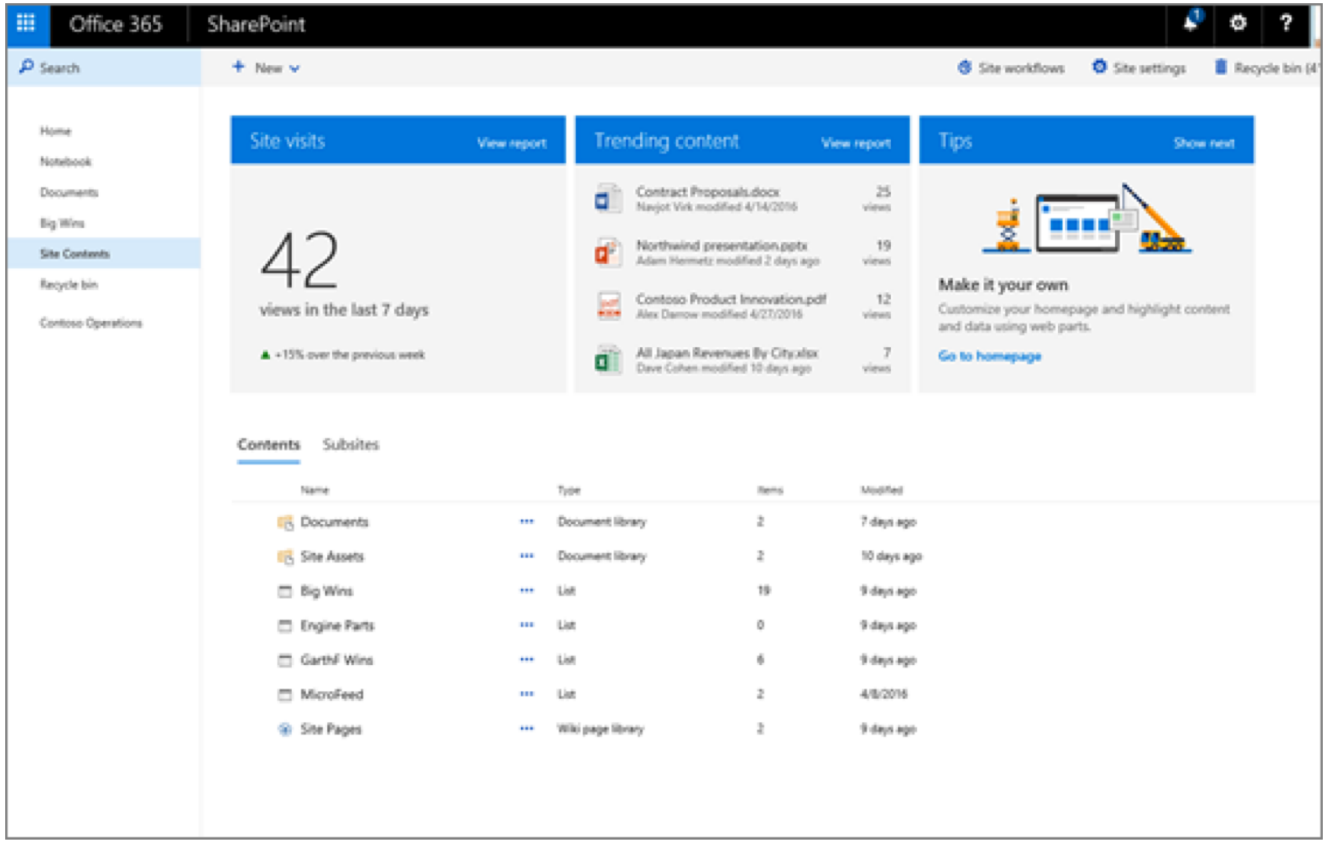
SUCCESS STORIES - DISSEMINATION

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



SUCCESS STORIES - DISSEMINATION

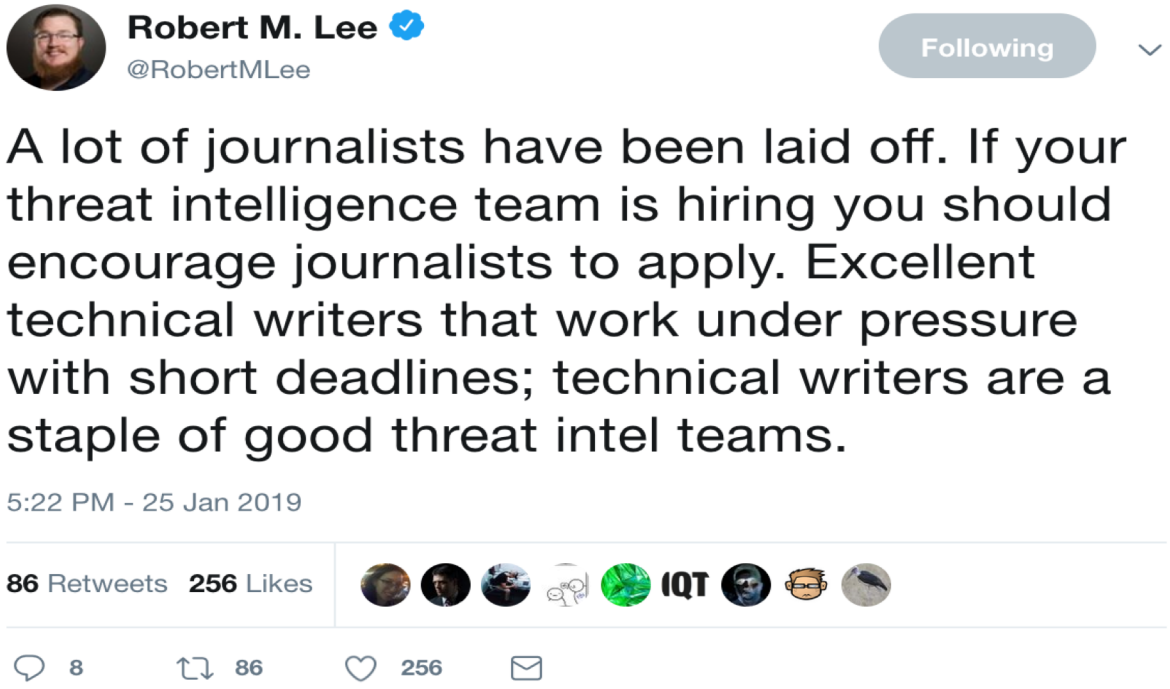
- Store the intel products in SharePoint
- Access control & Confidential reports
- Capture Site stats
- Measure outreach



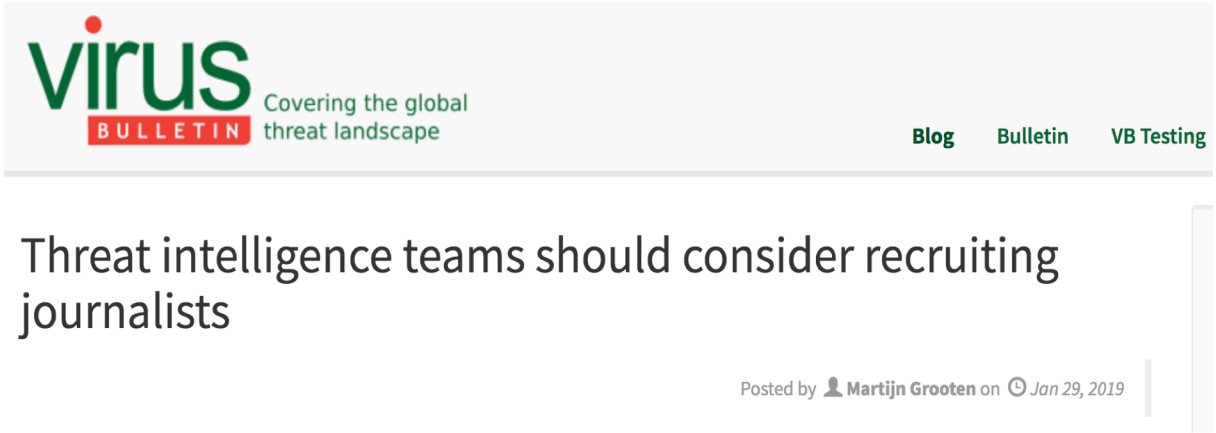
SharePoint

SharePoint Online

JOURNALISM & CTI



Reference:
Robert M. Lee



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

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

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%)"*

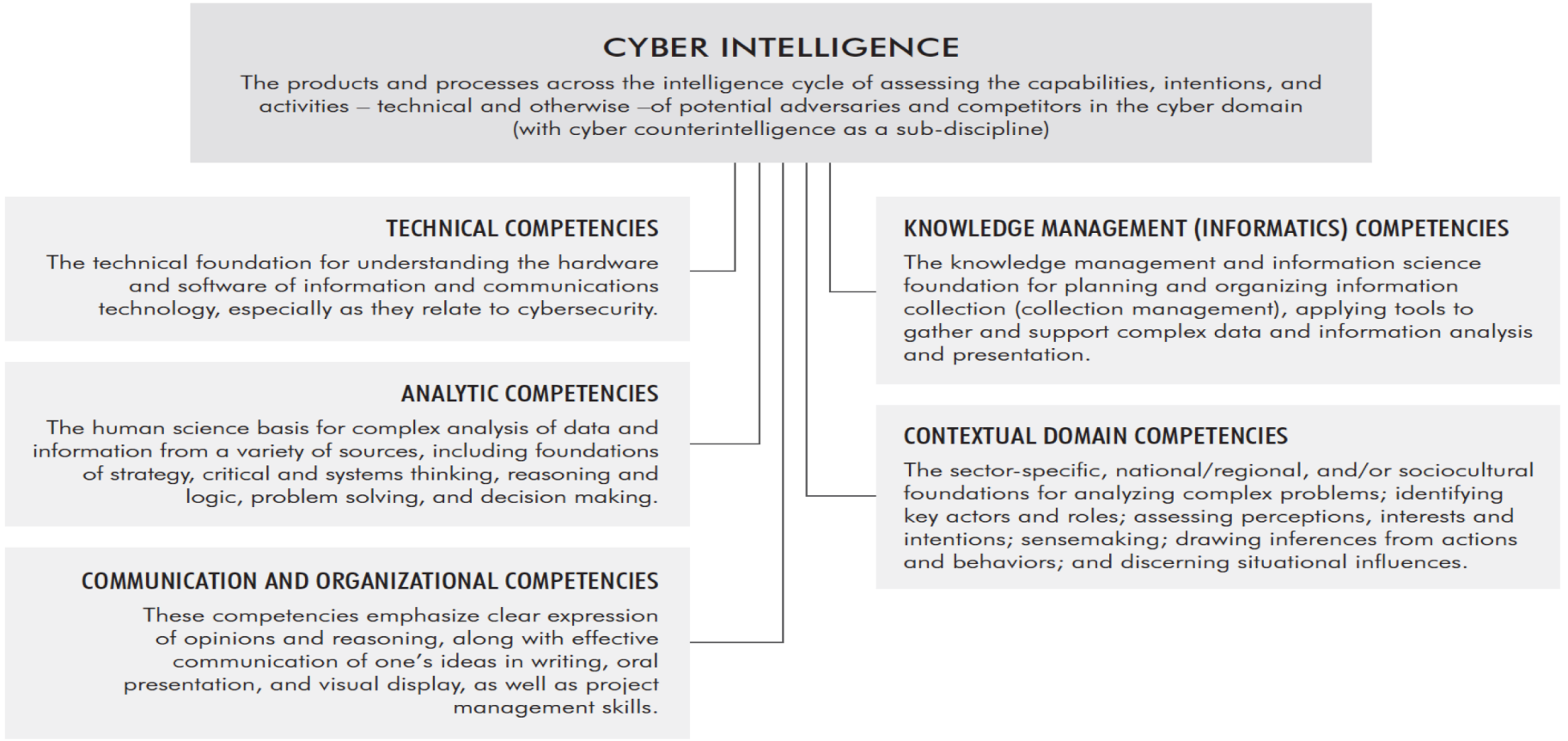
- Organizational challenges

- 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?"*

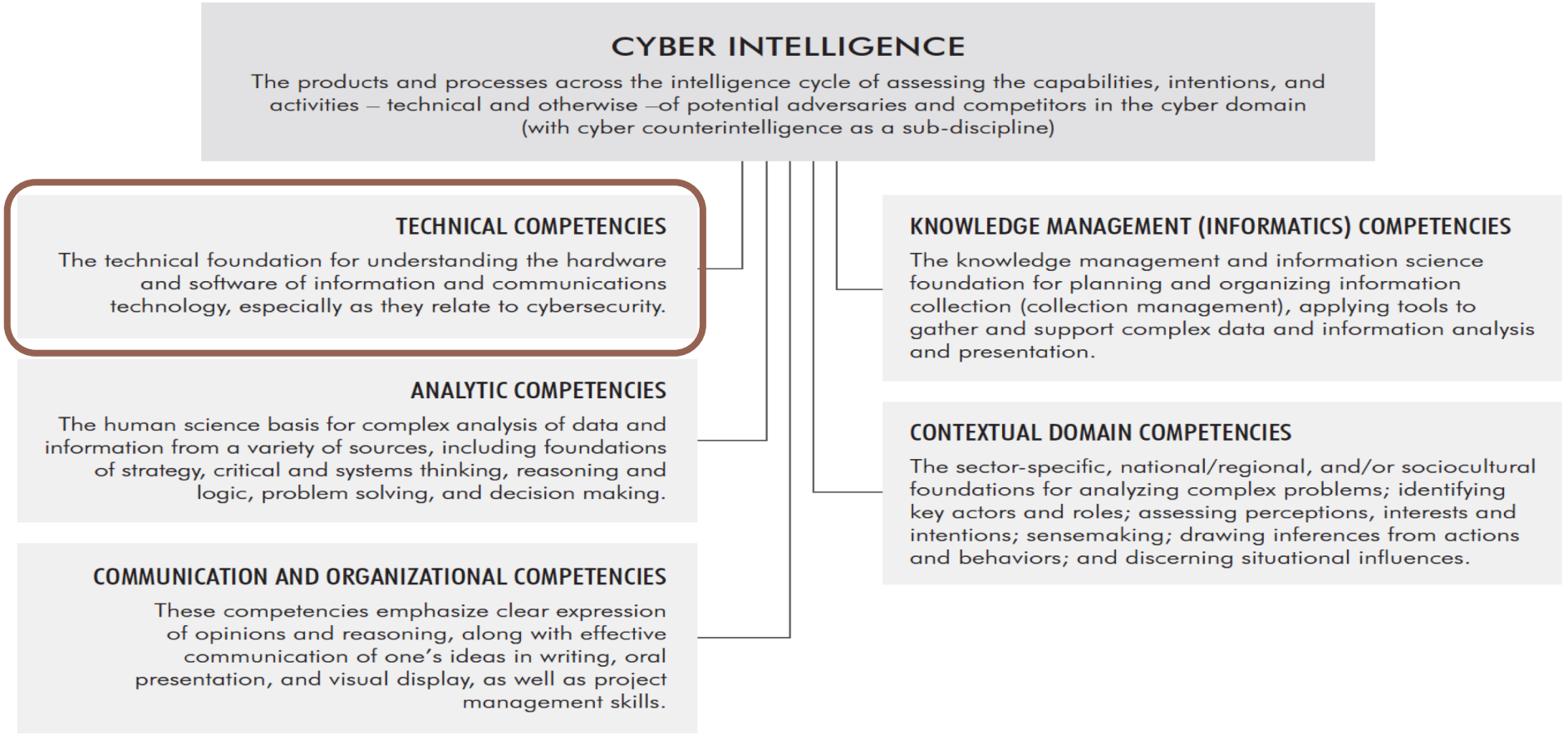
CTI ANALYST COMPETENCIES



Reference:

INSA
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

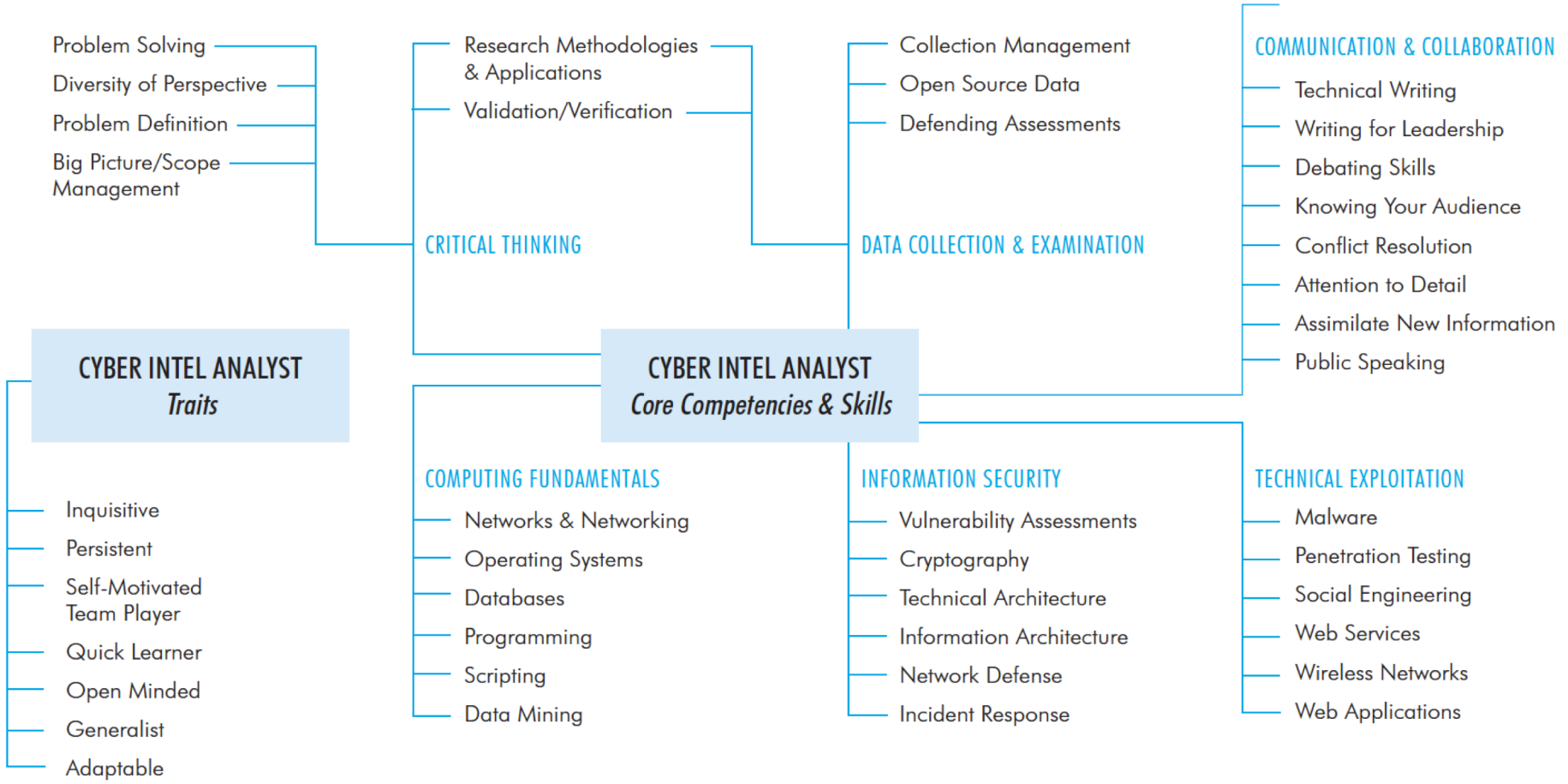
CTI ANALYST COMPETENCIES



Reference:

INSA
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

CTI ANALYST COMPETENCIES



Reference:

INSA
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

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 Intellgience: 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

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

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