A 5-YEAR LOOK BACK IN CTI PRACTICES

CTI-EU 2018

Andreas Sfakianakis

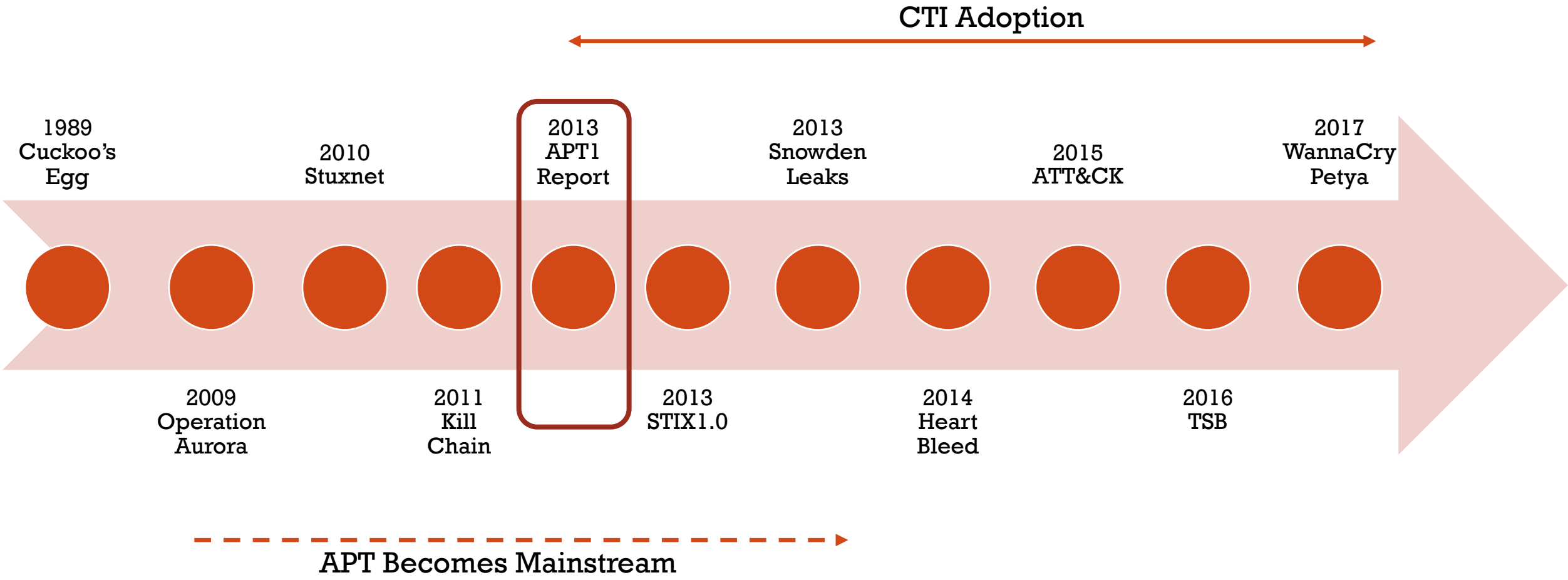
CTI Professional

WHO AM I

- CTI and IR professional in Financial and Oil & Gas sectors
- External Expert for ENISA and European Commission
- Member of CTI Working Groups: ENISA ETL SG, ENISA CTI CF, OASIS CTI-TC, FIRST CTI SIG, FIRST CTI 2019 PC, EC-Council CTI
- Website: www.threatintel.eu / Twitter handle: @asfakian

References for this presentation: http://bit.ly/cti-eu-2018

TIMELINE OF IMPORTANT EVENTS IN CTI

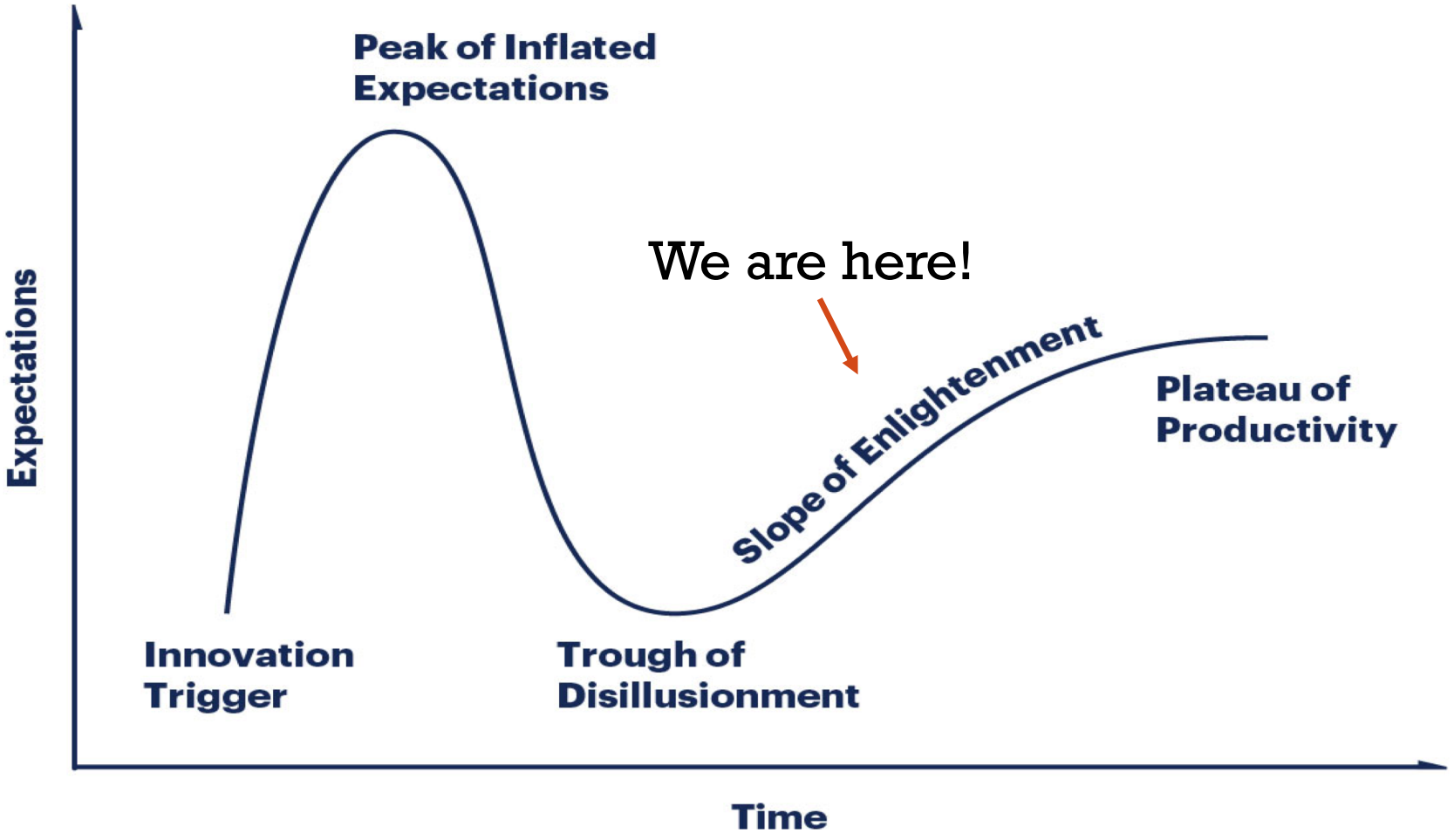


AS A COMMUNITY, WE DID GREAT PROGRESS!

	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 SCORED POORLY DURING THESE 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 are CTI teams contributing 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

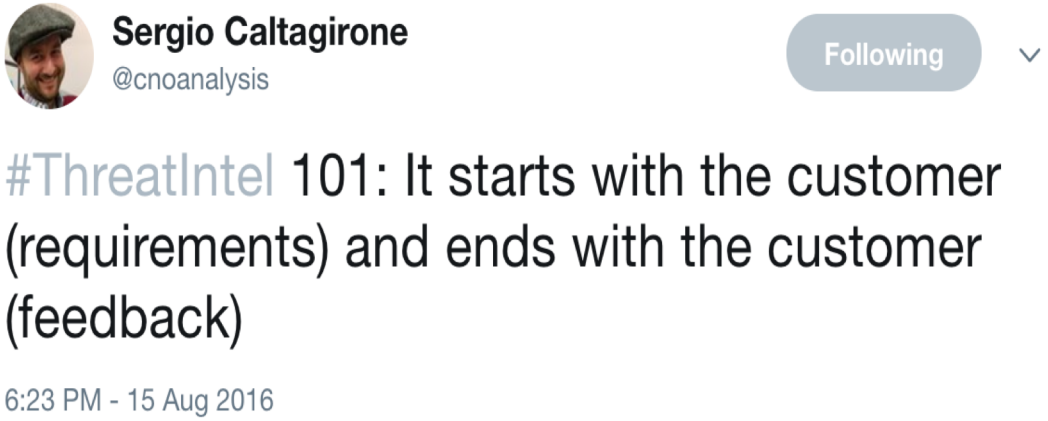
- Incident Responders
- Threat Hunters
- Vulnerability Management
- Red Team
- Fraud Team
- Sys Admins
- IT Managers

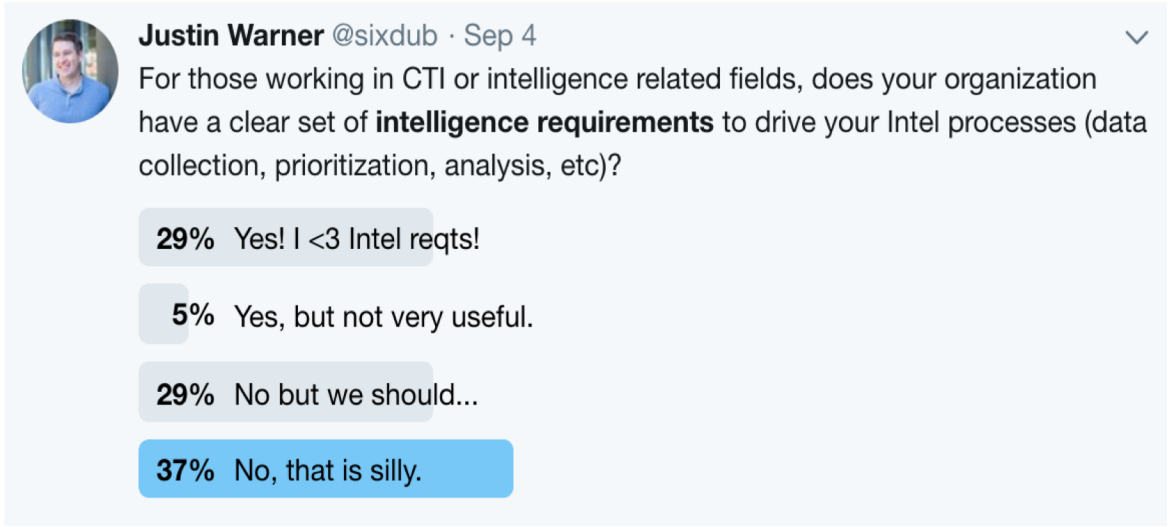
Strategic Intelligence

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

INTELLIGENCE REQUIREMENTS

- Intelligence requirements are enduring questions consumers of intelligence needs answers to.
- Answer critical questions intelligence customers/stakeholders care about (not what YOU care about).

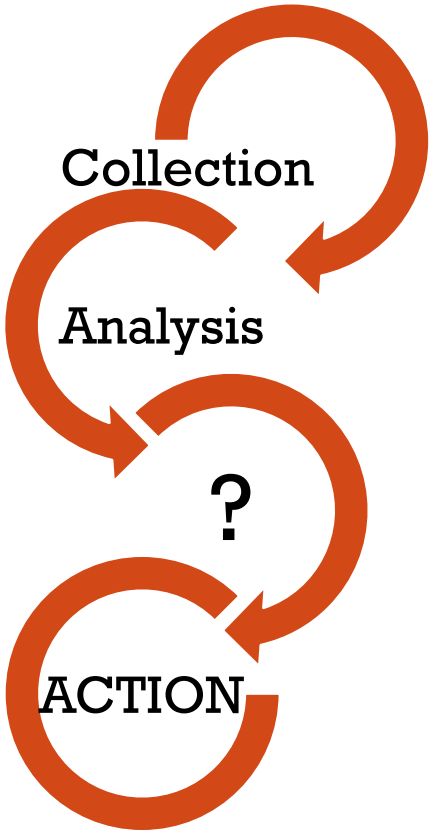




#2 FINALIZED REPORT AND DISSEMINATION

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

FINALIZED INTELLIGENCE PRODUCT



- Production requirements
- Reporting templates
- Style Guide
- IC Analytic Standards (ICD 203)
  - BLUF
  - What? So what? What next?
- Technology enablement

Reference:
Christian Paredes

#3 CTI ANALYST SKILLSET

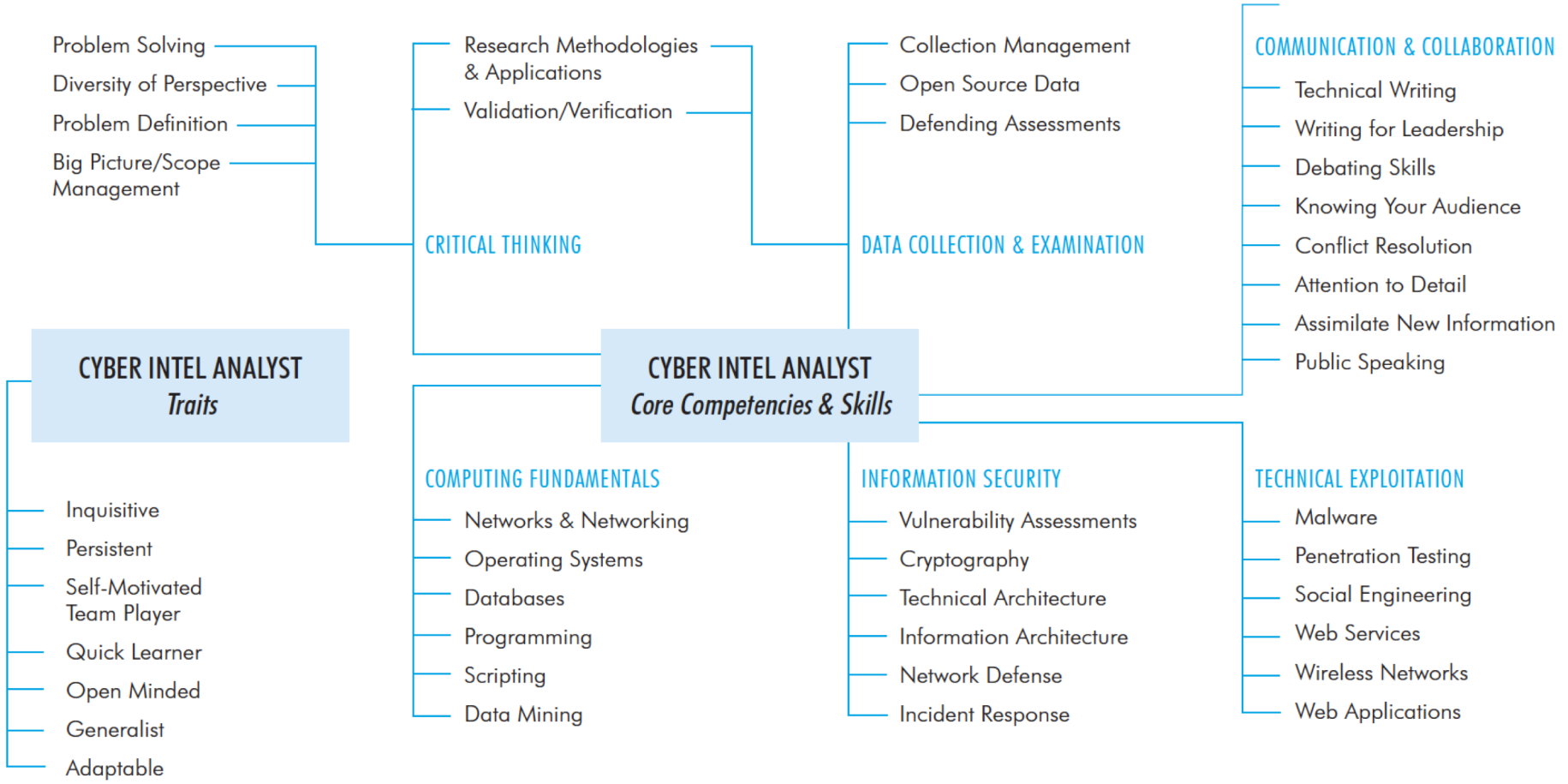
- CTI skills shortage
  - SANS CTI Survey 2018: "*62% of respondents cited a lack of trained CTI professionals and skills as a major roadblock, an increase of nearly **10 percentage points over 2017** (53%)*"

- Organisational challenges

- "The real successes in cyber security have been where **skills are continually upgraded**, **staff growth is moderate** and next-generation **cyber security tools are used to act as 'force multipliers'** that enable limited staff to keep up with the speed of both threats and business demands." - John Pescatore.

- Challenges for CTI teams

CTI ANALYST COMPETENCIES



Reference:

INSA
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

KEY TAKEAWAYS

- More focus should be put on implementing key areas of intelligence direction.
  - Reach out to your stakeholders
  - Define the operational environment/crown jewels
  - Start the discussion on intelligence requirements
- Intelligence dissemination and feedback is usually the weak link in our intelligence cycle.
  - Report writing as a critical CTI skill (for operational and strategic intelligence).
  - Cross-pollination - Intelligence tradecraft wasn't invented yesterday
- Focus on CTI analyst's skillset
  - Invest on internal/external CTI training opportunities
  - Use well established frameworks to assess your CTI team's skill coverage
  - Streamline BAU CTI activities, make them repeatable (e.g. playbooks, SOPs, etc.)
  - Build a working environment for knowledge sharing (e.g. review process, SAT exercises, etc.).

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

CTI-EU 2018

Andreas Sfakianakis

CTI Professional

Sharing is caring!

References for this presentation: http://bit.ly/cti-eu-2018