Current skills gap for capable CTI analysts: Training for forensics & analysis

WORKSHOP CTI – EU | Bonding EU Cyber Threat Intelligence

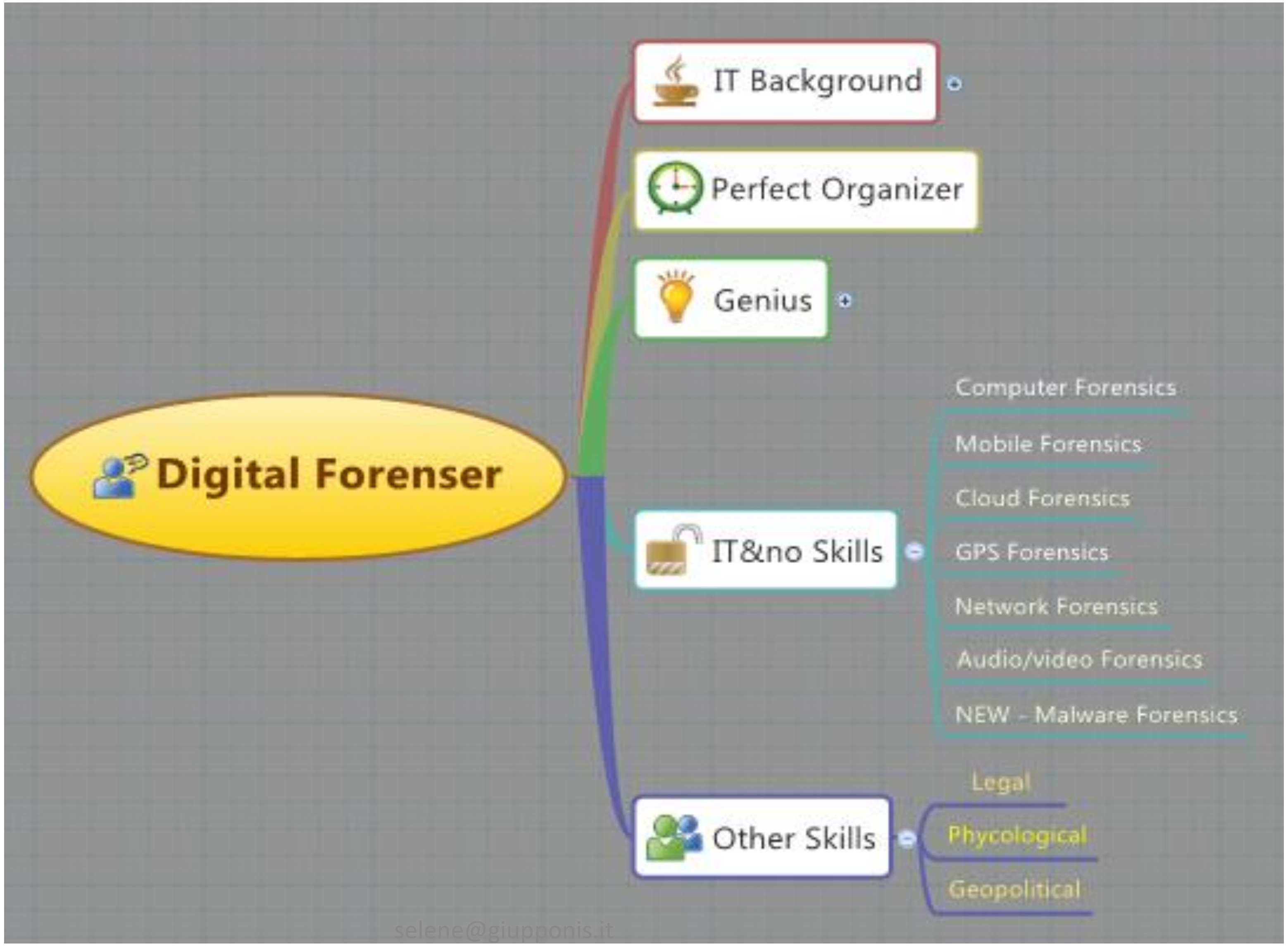
30-31 October, Link Campus University, Rome, Italy

Ing. Selene Giupponi – Cyber Security Advisor & Senior Digital Forensics Consultant

Who am I?

- Cyber Security Advisor & Senior Digital Forensics Consultant
- Computer Engineering Degree + Master in Computer Forensics & Digital Investigations
- Active Member of the IT Engineer Commission, Engineers Association of the Latina Province
- General Secretary and Member @ IISFA (INFORMATION SYSTEM FORENSICS ASSOCIATION, ITALIAN CHAPTER)
- Consultant for Law Enforcement
- Advisor @European Courage Focus Group – Cyber Terrorism & CyberCrime
- ITU Roster of Experts
- HTCC HIGH TECH CRIME CONSORTIUM Member
- Founder at Security Brokers ScpA
- Founder ECSO (European Cyber Security Organization)

Who’s the «IT Forensics expert», today?!?



Digital Forenser

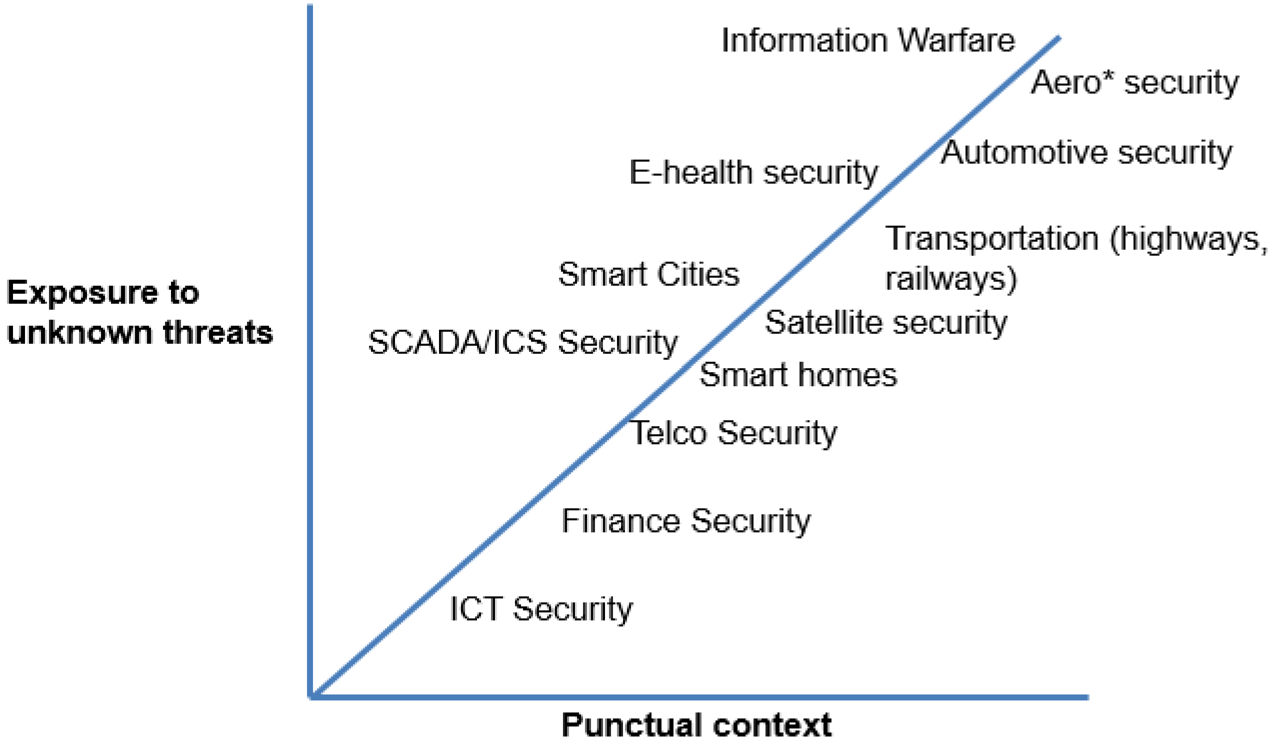
- IT Background
- Perfect Organizer
- Genius
- IT&no Skills
  - Computer Forensics
  - Mobile Forensics
  - Cloud Forensics
  - GPS Forensics
  - Network Forensics
  - Audio/video Forensics
  - NEW - Malware Forensics
- Other Skills
  - Legal
  - Phycological
  - Geopolitical

* Forensics Fields

- (Digital) Forensics
  - Host Forensics
    - MS Windows
    - *NIX/Linux
    - Mainframe
  - Network Forensics
  - Mobile Forensics
  - SCADA Forensics
  - Autmotive Forensics
  - GPS Forensics
  - Drones Forensics
  - IoT Forensics

Threats

Digital Forensics



Exposure to unknown threats

Information Warfare

Aero* security

Automotive security

E-health security

Transportation (highways, railways)

Smart Cities

Satellite security

SCADA/ICS Security

Smart homes

Telco Security

Finance Security

ICT Security

Punctual context

Cyber Threat Intelligence

Source:
Raoul Chiesa, Security Brokers

In every organization that uses Cyber Threat Intelligence, it is necessary to establish an interchange among those teams involved in Digital Investigations and Threat Intelligence analysis.

….Is that «enough»??

Cybersecurity Skills Gap

- **Size of the problem**
  - At least 1.5M cybersecurity jobs will be left vacant by 2019
  - 1 in 5 organization receives fewer than 5 candidates for each advertised security position and 37% of the organisations lament that fewer than 1 in 4 of the candidates they do receive are actually qualified for the job!
  - The cybersecurity skills shortage creates tangible risks to organizations, individuals and the nations

- **Lack of certified professionals**
  - The security job market has big gaps with regards to security certifications
  - The cost of training and cerfication is one of the underlying causes of the cybersecurity skills gap

- **Niche needs?**
  - High-value skills in critically short supply:

  ✓ Intrusion detection

  ✓ Secure software development

  ✓ Attack mitigation

  - Other desired skills include: malware analysis skills, familiarity with commercial tools and feeds, knowledge of adversaries campaigns and the ability to write correlation rules to link security events.

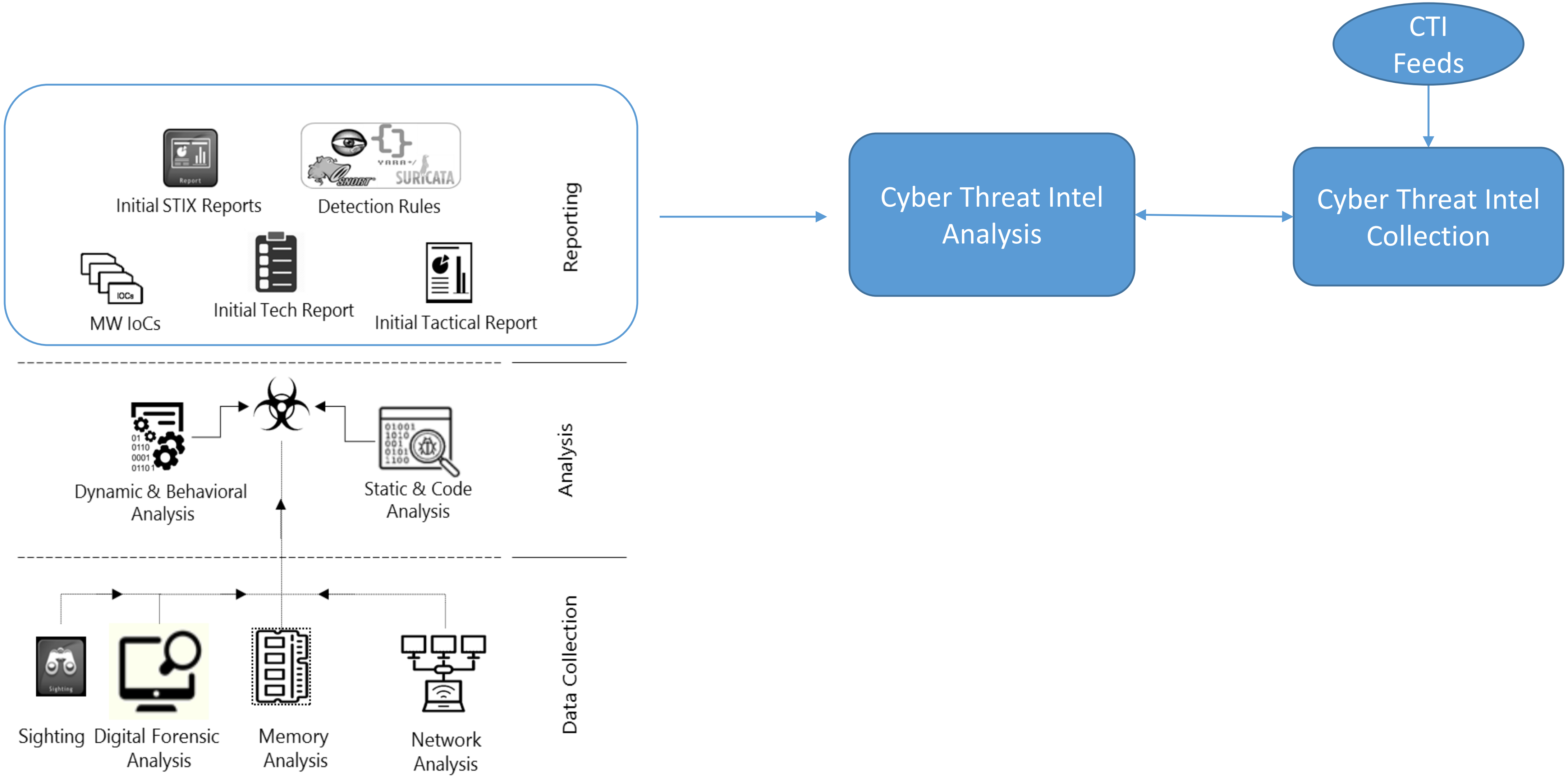
Overall recap + Recommendations

Challenge	Recommendations	Target
Lack of Competence Building Support	• Increasing government expenditure on cyber security training through matched funding and/or financial incentives; • Pushing for more cyber security programs in school and higher education.	Government
Lack of cyber security in Academia	• Partner with professional cyber security training vendors to offer extra extra-curriculum professional certifications and hands-on experience; • Organize Cyber Security Games and Competitions and/or facilitate students to participate.	Academia
Security Competition and Exercise	• Promoting gaming and technology exercises	Government
Companies Do not Invest Enough in Staff Training	• Shift spending from security systems to people and processes; • Develop better competence building programmes, which can be delivered by competent in-house staff and pay for staff certification attempts.	Organizations
Cost of Training and Certifications	• Develop better competence building programmes, which can be delivered by competent in-house staff and pay for staff certification attempts.	Government, Academia and Organizations
Lack of Adequate Training	• Prioritize formal and structured training over online/self-learning especially to begin with	ALL
Young Professional Not Doing It Right!	• Follow a goal-oriented approach to produce tangible deliverables at every step of the learning process	Individuals

CTI Analysts vs Forensics Analysts

- Investigations and Evidences
- Proactive vs Post Incidents
- CTI is a useful source of information to support Digital Forensics Analysts

Let’s brainstorm!



Initial STIX Reports

Detection Rules

MW IoCs

Initial Tech Report

Initial Tactical Report

Reporting

Dynamic & Behavioral Analysis

Static & Code Analysis

Analysis

Sighting

Digital Forensic Analysis

Memory Analysis

Network Analysis

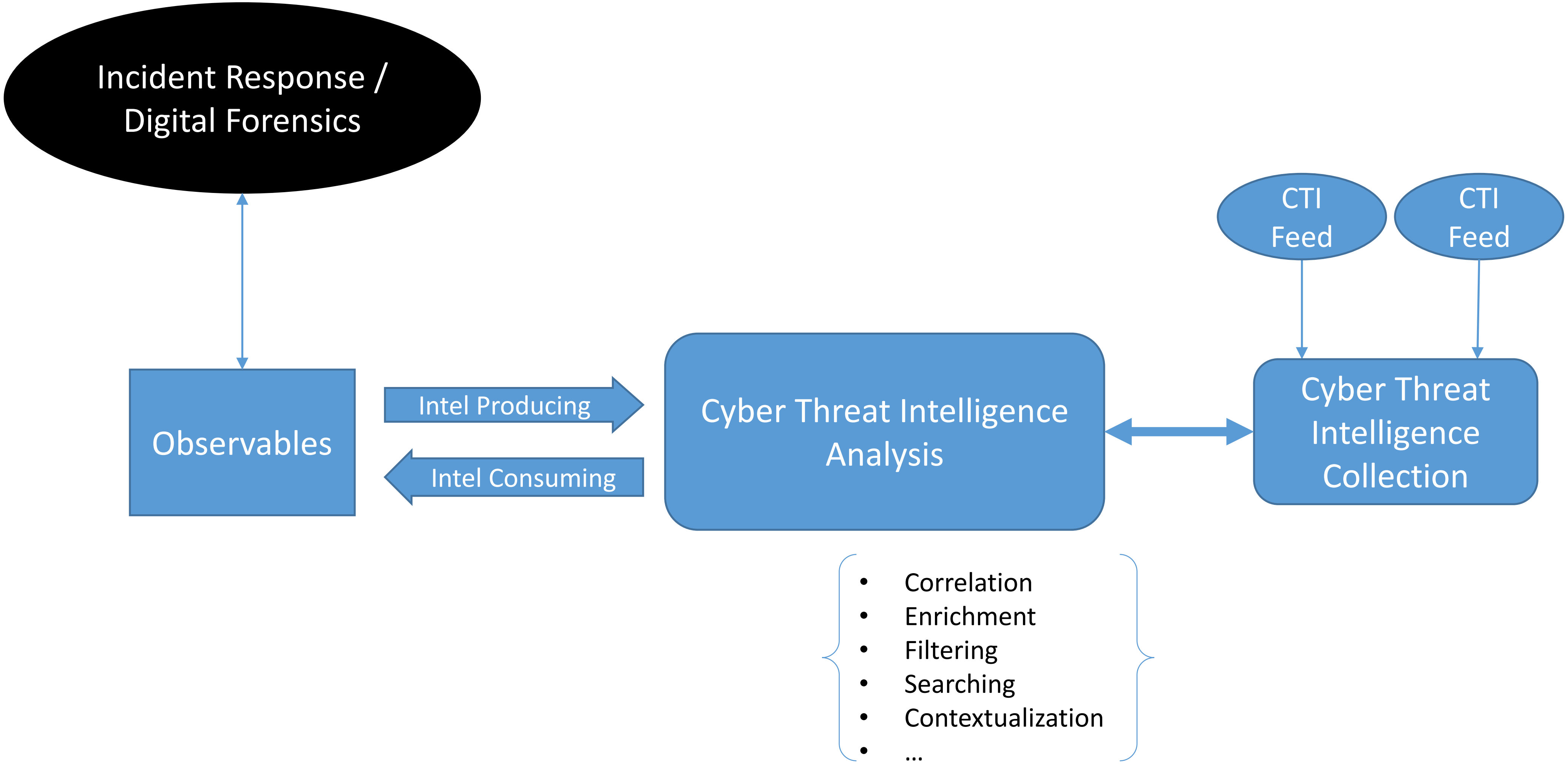
Data Collection

Cyber Threat Intel Analysis

Cyber Threat Intel Collection

CTI Feeds

Let’s brainstorm!

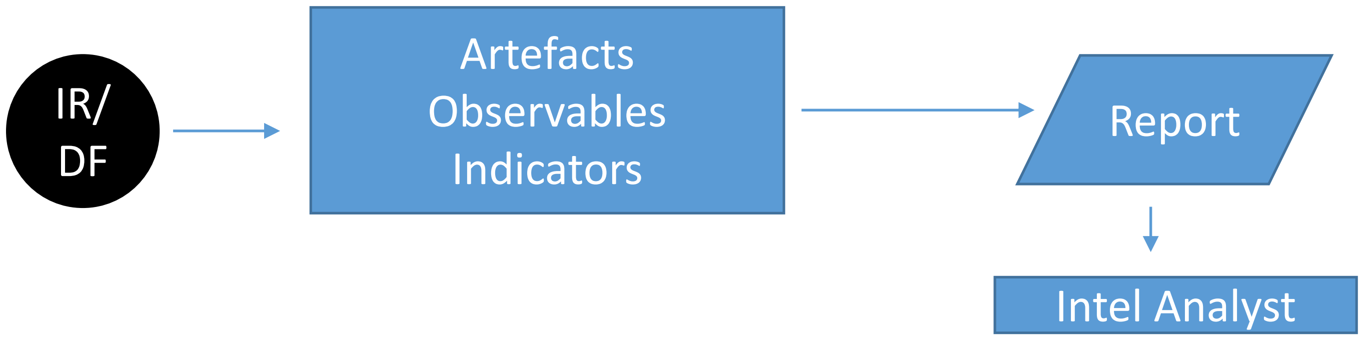

Incident Response / Digital Forensics
CTI Feed
CTI Feed
Observables
Intel Producing
Intel Consuming
Cyber Threat Intelligence Analysis
Cyber Threat Intelligence Collection

- Correlation
- Enrichment
- Filtering
- Searching
- Contextualization
- …

Intel Production

Let’s brainstorm!

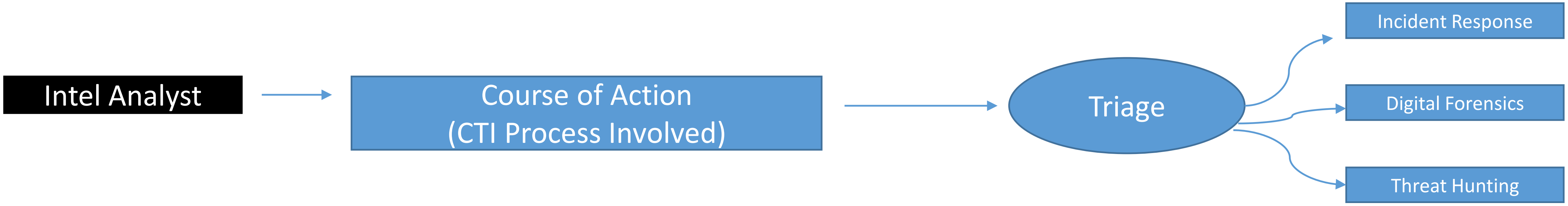
- Through Digital Investigation we can identified and detect the compromised elements.
- These observable, if sent to Threat Intelligence analysis, can be contextualized and provide more information to extend (make it more efficient) the scope of the investigation. In this case, Digital Forensics Team will produce Threat Intelligence.



Let’s brainstorm!

Intel Consuming

- Starting from intelligence analysis, key information can be provided to teams called to do triage activities to investigate on possible compromises. In this case, the Digital Forensics team uses Cyber Threat Intelligence for investigation.



The challenge of Corporate Training

Inadequate levels of Training

- Companies often decide **not to train their staff** for fear they may leave once the training is over.
- Companies prefer to invest in systems and technologies under the belief those will remain as an asset to the company even after the employees leave.
- ROI on security training is difficult to measure.
- Training costs money, period!
- Lack of continuous training on business procedures and processes prevents the best team collaboration and does not allow to enhance the internal skills to deal effectively a risk.
- …

The challenge of Corporate Training

- Not all organizations in which CTI has been introduced have jointly developed processes integrating operations and communications between Secure operation teams and CTI teams.
- The ways of disseminating within the teams involved in CTI processes need to be improved.
- Digital Forensics analysts do not yet have a clear understanding of the integration of Threat Intelligence information into Digital Forensics methodologies.
- Digital Forensics analysts should be trained on the main forms of Intelligence information representation in order to make dissemination faster and more effective
- CTI Analysts and Forensics Analysts training program together into the same Organization.

Contacts

- Eng. Selene Giupponi

selene@giupponis.it

- Twitter: @SeleneGiupponi
- Linkedin: https://it.linkedin.com/in/selenegiupponi
- PGP Key – ASK ME!